INTERNAL POLICIES

This document outlines the internal policies of Live Now Technology SLU. These policies are designed to ensure a safe, secure, and high-quality work environment while adhering to legal and regulatory requirements.

Code of Conduct

Live Now Technology SLU is committed to maintaining the highest standards of **ethics, professionalism, and corporate responsibility**. This Code of Conduct applies to all employees, contractors, and business partners, ensuring a fair, inclusive, and legally compliant workplace.

1. Ethical Business Practices

At **Live Now Technology SLU**, we believe that ethics and transparency are the foundation of sustainable business success. All our decisions and actions must be guided by **principles of honesty, responsibility, and fairness**, ensuring that our operations are **just, legal, and aligned with the highest ethical standards**.

All employees, executives, and business partners must adhere to the following ethical business conduct guidelines:

1.1 Compliance with Laws and Regulations

Live Now Technology SLU operates within an international framework, making legal and regulatory compliance a top priority.

- All employees must **understand and comply with local, national, and international laws** relevant to their work.
- Regulations from international entities such as the **European Union (EU), the Spanish Data Protection Agency (AEPD), and the Organisation for Economic Co-operation and Development (OECD)** must be followed.
- The company will provide **regular training on ethics and compliance** to ensure that all employees remain up to date with applicable legal requirements.

1.2 Anti-Corruption and Anti-Bribery Policy

Corruption and bribery pose serious threats to business integrity. At Live Now Technology SLU, we enforce a **zero-tolerance policy** against any form of corruption.

- It is **strictly prohibited to offer, promise, solicit, or accept bribes** in any business transaction.
- Employees must **not make improper payments** to government officials, clients, suppliers, or other stakeholders.
- If corruption is suspected, employees must report it immediately through the **internal anonymous reporting mechanism**.
- The company will conduct periodic **financial audits** to identify risks related to corruption.
- **Facilitation payments** (small payments to expedite administrative processes) are not permitted.

🚨 **Example of misconduct:** An employee offers a "special commission" to a government official to speed up the approval of an operating license. This is an illegal act that will result in **disciplinary and legal consequences**.

1.3 Conflict of Interest

Employees and executives of Live Now Technology SLU must **make decisions based on the company's best interests**, avoiding situations where **personal gain or third-party benefits interfere with their professional responsibilities**.

- A **conflict of interest** arises when an employee's personal interests **could influence their judgment**.
- Employees must **disclose any personal or financial relationship** with suppliers, clients, or competitors that may impact their objectivity.
- Employees are prohibited from **holding simultaneous employment with competitors** or **accepting valuable gifts** from clients or suppliers.
- The company provides a mechanism to **report and manage potential conflicts of interest transparently**.

💡 **Example of a conflict of interest:** An employee responsible for selecting a software provider recommends their sibling's company for the contract. Before proceeding, they must **disclose this relationship** to Human Resources to prevent biased decision-making.

1.4 Fair and Transparent Competition Practices

Live Now Technology SLU promotes **free and fair market competition**, avoiding any **unfair or monopolistic practices**.

- Any **collusion or price-fixing agreements** with competitors are **strictly prohibited**.
- Employees must not share **confidential pricing, customer, or strategy information** with industry competitors.
- Intellectual property rights must be respected, and **competitor information should not be obtained unlawfully**.
- Business relationships with clients and suppliers must be **transparent and include clear terms and conditions**.

📌 **Example of prohibited conduct:** Two competing tech companies agree **not to compete in specific markets** to maintain high prices. This practice is illegal and a violation of **fair competition laws**.

1.5 Ethical Relationships with Clients and Suppliers

Business relationships must be based on **transparency, fairness, and mutual respect**.

- Contracts must be **clear, fair, and free from misleading or abusive clauses**.
- Agreed payment terms with suppliers and clients must be **strictly followed**.
- Employees must **not pressure suppliers into offering uncompetitive prices**.
- The selection of suppliers must follow **objective and documented criteria**, avoiding favoritism or personal bias.

Example of ethical business conduct: Before signing a contract with a software provider, a company director **reviews multiple options** on the market and chooses the most suitable one based on **quality, price, and service**.

1.6 Responsible Use of Information and Data Protection

Company information must be handled with **confidentiality and responsibility**.

- Employees must **safeguard sensitive business and client information**.
- The company complies with the **General Data Protection Regulation (GDPR)** for the processing of personal data.
- Confidential information must not be shared with third parties **without explicit authorization**.
- Employees must avoid transmitting sensitive data **through unsecured channels**.

- Employees must use **strong passwords and multi-factor authentication (MFA)** on company devices.

🔒 **Example of a data protection violation:** An employee downloads **sensitive client data** to their personal computer without authorization. This is a serious **GDPR violation** and a **security risk**.

1.7 Ethical Compliance Audits and Monitoring

Live Now Technology SLU conducts **internal audits** to ensure compliance with ethical business practices.

- Regular inspections and controls are performed to **identify risks and potential violations**.
- Employees must **fully cooperate** with audits and provide accurate information.
- Any irregularities found will be reviewed by the **Ethics Committee**, which will implement necessary corrective actions.

📊 **Example of an internal audit:** The compliance team **reviews recent contracts** with suppliers to ensure that **procedures have been followed correctly** and that there are **no conflicts of interest**.

Conclusion

At **Live Now Technology SLU**, we are all responsible for ensuring that **business practices are ethical, transparent, and legally compliant**. Our commitment to integrity is essential for **building a solid, trustworthy, and respected company in the technology sector**.

2. Workplace Conduct & Respect for Others

At **Live Now Technology SLU**, we are committed to fostering a professional, inclusive, and respectful work environment where all employees feel safe, valued, and empowered to contribute to our collective success. **We believe that a positive and ethical workplace culture is essential for employee well-being, productivity, and overall organizational growth.**

This section establishes the guidelines and expectations for workplace conduct, emphasizing mutual respect, fairness, and adherence to ethical behavior in all professional interactions.

2.1 Commitment to a Professional and Inclusive Work Environment

Live Now Technology SLU is dedicated to creating a **workplace free of discrimination, harassment, and intimidation**. We expect every employee, contractor, and business partner to act with **respect, integrity, and professionalism** at all times.

- **Respect for Diversity and Inclusion:** We celebrate diversity and believe that an inclusive workplace fosters creativity, innovation, and excellence. Discrimination **based on race, gender, age, disability, sexual orientation, religion, nationality, or any other characteristic** is strictly prohibited.
- **Equal Opportunity Employment:** All employment decisions—such as hiring, promotions, salary increases, and training—must be based **purely on merit, performance, and qualifications** without bias.
- **Cultural Awareness:** Employees working in a global or multicultural environment must remain mindful of **cultural differences** and practice respect in all professional interactions.

Example of positive workplace conduct: A hiring manager ensures that all job candidates are evaluated **based on skills and experience**, rather than personal characteristics such as gender or nationality.

✕ **Example of inappropriate behavior:** A senior employee consistently **ignores** the input of a younger colleague based on age-related bias. This is unacceptable and must be reported.

2.2 Anti-Harassment and Anti-Bullying Policy

Harassment, bullying, and any form of workplace hostility are **strictly prohibited** at Live Now Technology SLU. We define harassment as **any unwelcome behavior that creates an intimidating, hostile, or offensive work environment**.

- **Sexual Harassment:** Unwanted advances, inappropriate jokes, suggestive comments, or any behavior of a sexual nature that **makes an employee uncomfortable** will not be tolerated.
- **Verbal and Physical Harassment:** Insulting language, offensive gestures, aggressive behavior, or threats are not acceptable in any circumstance.
- **Cyberbullying and Digital Harassment:** Employees must not engage in **online harassment**, including offensive emails, public shaming, or inappropriate messages on communication platforms (Slack, Teams, etc.).
- **Escalation Procedures:** If an employee feels they have been harassed or bullied, they must report the issue through the **Internal Employee Communication Channel (Anonymous Reporting Mechanism)** for immediate investigation.

🚨 **Example of workplace harassment:** A manager **makes repeated comments** about an employee’s physical appearance in a way that makes them uncomfortable. This must be reported to HR immediately.

2.3 Workplace Relationships & Professionalism

- **Maintaining Professional Boundaries:** While friendly relationships are encouraged, employees must **maintain professional conduct at all times** and avoid **excessive familiarity or favoritism** in the workplace.
- **Avoiding Conflicts of Interest in Workplace Relationships:** Employees engaged in **romantic or personal relationships** with colleagues or managers **must disclose the relationship** if it creates a conflict of interest.
- **Professional Communication:** All internal and external communications must be conducted in a **courteous, respectful, and constructive manner**—whether in emails, meetings, or online collaboration tools.
- **Dress Code and Professional Appearance:** Employees must present themselves in a way that reflects **professionalism and respect for the workplace environment**. While we allow flexibility, employees should follow **company guidelines** regarding appropriate dress standards.

Example of professional behavior: During a disagreement in a meeting, two employees **discuss their differing opinions with respect and professionalism**, rather than raising their voices or making personal attacks.

❌ **Example of unprofessional conduct:** An employee frequently **interrupts and dismisses** colleagues in team discussions, creating a **hostile work environment**.

2.4 Workplace Safety & Health

The health and safety of employees are of **utmost importance** to Live Now Technology SLU. We are committed to providing a **safe, hazard-free work environment** and promoting **physical and mental well-being**.

- **Compliance with Safety Regulations:** Employees must **adhere to safety protocols** and report any hazardous conditions or safety risks immediately.
- **Emergency Preparedness:** Employees must familiarize themselves with **emergency procedures, fire exits, and first-aid resources** available in the workplace.
- **Mental Health & Well-being:** The company promotes work-life balance and encourages employees to **seek support** for any mental health concerns. **Burnout prevention measures**, including reasonable workload distribution and wellness initiatives, are actively supported.
- **Alcohol and Substance Abuse Policy:** The consumption of alcohol or illegal substances **during work hours or on company premises** is strictly prohibited, except during official company events where alcohol may be permitted in a **responsible manner**.

🚨 **Example of a workplace safety violation:** An employee **fails to report a loose electrical wire**, leading to a safety hazard that could have been prevented.

2.5 Workplace Confidentiality & Data Protection

Employees must **handle company information responsibly** and protect sensitive data from unauthorized access.

- **Confidentiality Agreement:** Employees must not disclose **company trade secrets, financial data, client information, or project details** without proper authorization.
- **Proper Use of IT Systems:** Employees must use **corporate devices, emails, and software platforms** responsibly and avoid exposing company systems to security risks.

- **Remote Work Security:** Employees working remotely must **secure their work environment**, use **VPNs, encrypted communication**, and avoid **public Wi-Fi** for handling company data.
- **Reporting Data Breaches:** If an employee suspects a **data breach or security vulnerability**, they must report it immediately to the **IT Security Team**.

🔒 **Example of a data protection violation:** An employee downloads company files **onto a personal USB drive** and later loses it, exposing sensitive business information. This is a **serious security risk**.

2.6 Conflict Resolution & Workplace Disputes

Workplace disagreements are inevitable, but they must be resolved in a **professional and constructive manner**.

- **Encouraging Open Dialogue:** Employees are encouraged to communicate openly and address **concerns directly** before escalating disputes.
- **Use of Mediation Services:** If conflicts persist, HR can facilitate a **neutral mediation process** to find an appropriate resolution.
- **Zero Tolerance for Retaliation:** Employees must **never face retaliation** for reporting a workplace concern or dispute.

Example of proper conflict resolution: Two team members have a disagreement over a project's direction but **schedule a meeting** to discuss solutions calmly and collaboratively.

✖ **Example of improper behavior:** An employee **spreads negative rumors** about a colleague following a workplace disagreement, instead of resolving the issue professionally.

Conclusion

At **Live Now Technology SLU**, our workplace culture is based on **mutual respect, professionalism, and inclusivity**. Every employee has a responsibility to **contribute to a positive work environment**, ensuring that our workplace remains a space where talent, innovation, and teamwork thrive.

3. Data Protection & Confidentiality

At **Live Now Technology SLU**, we recognize that **data is one of our most valuable assets** and that protecting sensitive information is fundamental to maintaining trust, ensuring business continuity, and complying with legal and regulatory requirements. We are committed to safeguarding **personal, client, and company data** in compliance with **GDPR (General Data Protection Regulation)** and other applicable laws.

This section outlines our **policies, responsibilities, and best practices** regarding the collection, handling, storage, and sharing of information within the company.

3.1 Compliance with Data Protection Laws (GDPR & Other Regulations)

Live Now Technology SLU strictly adheres to the **GDPR**, which governs the collection, processing, storage, and transfer of **personal and corporate data** within the European Union.

🔹 **Key Principles of Data Protection (as per GDPR):**

1. **Lawfulness, Fairness, and Transparency:** Data must be collected and processed **legally and transparently**.
2. **Purpose Limitation:** Information can only be used for **legitimate business purposes**.
3. **Data Minimization:** Only the **necessary amount of data** should be collected and stored.
4. **Accuracy:** Data must be **kept up to date** and corrected if inaccurate.
5. **Storage Limitation:** Personal data should **not be retained longer than necessary**.
6. **Integrity & Confidentiality:** Data must be **protected against unauthorized access and cyber threats**.
7. **Accountability:** The company must demonstrate **compliance with data protection policies** at all times.

⚠ **Example of a data protection violation:** An employee collects personal information from clients and later shares it with a third party **without consent**—this is a **GDPR breach**.

3.2 Employee Responsibilities in Data Protection

All employees must ensure **the confidentiality, integrity, and security of company and client data**.

Mandatory Employee Responsibilities:

- **Handle sensitive data carefully**: Employees must avoid exposing or misusing company data.
- **Use secure storage methods**: Physical and digital records must be **stored securely** (e.g., encrypted files, locked cabinets).
- **Report data breaches**: If an employee suspects **unauthorized access, leaks, or breaches**, they must report it **immediately** to IT Security.
- **Follow access control policies**: Employees must **not share passwords or access credentials** with unauthorized individuals.
- **Dispose of data securely**: Documents and files containing sensitive data must be **properly deleted or shredded** when no longer needed.

🚨 **Example of employee misconduct:** An employee **prints confidential client contracts and leaves them unattended** on a shared office desk.

3.3 Handling of Personal & Client Data

Client and employee personal data must be handled with **utmost care** and in compliance with GDPR.

🔐 **Rules for Handling Personal Data:**

- Collect and process data **only with explicit consent**.
- Use personal data **only for the purpose for which it was collected**.
- Implement **encryption and access controls** when storing personal information.
- Limit data access **only to authorized personnel**.
- Anonymize or pseudonymised data whenever possible to reduce risk.

📌 **Example of compliant behavior:** A marketing team **asks for explicit consent** before adding a customer’s email to a mailing list.

❌ **Example of a GDPR violation:** An HR employee **shares a colleague’s salary information** with an unauthorized person.

3.4 Secure Communication & IT System Usage

Employees must **follow best practices for secure communication** and ensure that all corporate IT systems are **protected against cyber threats**.

🖳 **IT Security Guidelines:**

- Use **strong passwords** and update them regularly.
- Enable **multi-factor authentication (MFA)** for email, databases, and cloud services.
- Do not open **suspicious emails or attachments** that may contain phishing attempts.
- Store company files only in **authorized locations (e.g., encrypted cloud storage, company servers)**.
- Use company-approved VPNs for **remote access** to internal systems.

⚠ **Example of IT security risk:** An employee **downloads confidential files onto a personal laptop** that lacks security measures, making it vulnerable to cyberattacks.

3.5 Confidentiality Obligations & Non-Disclosure Agreements (NDAs)

All employees are **legally required to maintain confidentiality** regarding company and client information.

📜 **Key Rules of Confidentiality:**

- Do not discuss **confidential company matters** in public places or unauthorized settings.
- Do not disclose sensitive information to **friends, family, or competitors**.
- Employees **must sign an NDA (Non-Disclosure Agreement)** before accessing confidential data.
- Breaching confidentiality obligations may lead to **disciplinary action, termination, and legal consequences**.

🚨 **Example of a confidentiality breach:** An employee **leaks business strategies** to a competitor in exchange for personal gain. This is grounds for **immediate termination and legal action**.

3.6 Data Breach Reporting & Incident Response

In the event of a **data breach**, employees must act **quickly and responsibly** to minimize risk and prevent further damage.

🚨 **Immediate Steps in Case of a Data Breach:**

1. **Report the breach** immediately to the **Data Protection Officer (DPO)** or IT Security.
2. **Secure the affected data** and attempt to **contain the breach** (e.g., revoke unauthorized access).
3. **Assist in the investigation** by providing relevant details and cooperating with internal security teams.
4. **Follow GDPR notification requirements** if the breach involves personal data (clients or employees).

📌 **Example of a proper response:** An employee **notices unauthorized access** to sensitive project files and **immediately reports it to IT Security**, preventing further exposure.

3.7 Third-Party Data Handling & Vendor Security

When working with **external vendors, consultants, or partners**, Live Now Technology SLU ensures that third parties comply with **our data security standards**.

🔍 **Third-Party Data Protection Requirements:**

- Vendors must **sign a Data Processing Agreement (DPA)** before handling company data.
- Third-party access to company systems must be **limited and monitored**.
- All external service providers must meet **industry security standards** and **GDPR compliance**.

Example of good practice: Before working with a cloud storage provider, the company **reviews their security policies** and ensures they comply with **ISO 27001 and GDPR**.

3.8 Employee Training & Awareness Programs

Live Now Technology SLU conducts **mandatory data protection training** to ensure all employees understand their responsibilities in handling data securely.

📌 **Training Topics Include:**

- GDPR compliance and legal requirements.
- Recognizing and preventing cybersecurity threats (e.g., phishing, malware).
- Best practices for secure data storage and sharing.
- Proper use of corporate email and communication tools.

📖 **Example of security awareness:** An employee **recognizes a phishing email** attempting to steal login credentials and reports it to IT Security before any harm is done.

Conclusion

At **Live Now Technology SLU**, protecting confidential information is **everyone's responsibility**. Employees must **follow these policies strictly** to safeguard company assets, maintain client trust, and **comply with GDPR regulations**.

4. Use of Company Resources

At **Live Now Technology SLU**, we recognize that **company resources** are critical assets that enable us to operate efficiently, innovate, and deliver high-quality services. Every employee has a responsibility to **use these resources responsibly, ethically, and in alignment with the company's goals**. This section provides clear guidelines on how employees must handle **technology, intellectual property, and sustainability efforts** to ensure the integrity and efficiency of our operations.

4.1 Responsible Use of Company Assets

Company assets, including **physical equipment, IT systems, software, and intellectual property**, are provided for **business-related purposes only**. Employees must respect and protect these assets to prevent loss, theft, damage, or misuse.

🔹 **General Rules for Company Asset Usage:**

- **Use resources efficiently**: Do not waste materials, electricity, or office supplies.
- **Protect company equipment**: Keep computers, devices, and tools secure from damage or loss.
- **Report misuse or theft immediately**: Notify management if you suspect any unauthorized use or security breach.
- **Maintain professionalism**: Company resources should be used in ways that align with corporate values and ethical standards.

🚨 **Example of misconduct:** An employee **takes home company equipment** (e.g., a laptop) for personal use without permission, violating company asset policies.

Example of compliance: An employee **locks their workstation** when leaving their desk to prevent unauthorized access.

4.2 Technology & IT Systems

IT systems, including **company computers, networks, software, and cloud services**, must be used strictly for **legitimate business purposes**. Employees are required to follow **cybersecurity best practices** to protect company systems from **unauthorized access, malware, and data breaches**.

🔐 **IT Security & Acceptable Use Policy:**

- **Use strong passwords**: Employees must set **unique and complex passwords** for all company systems and enable **multi-factor authentication (MFA)** where applicable.
- **Do not install unauthorized software**: All software must be approved by the IT department.
- **Prohibited activities**: Employees must not access, download, or share **illegal, offensive, or inappropriate content** using company devices or networks.
- **Report suspicious activity**: If an employee notices a **phishing email, malware infection, or security threat**, they must report it to IT Security immediately.
- **Limit personal use**: While minimal personal use of company IT resources may be tolerated, excessive or inappropriate use is prohibited.

⚠ **Example of a security violation:** An employee **downloads unauthorized software** onto a company laptop, exposing the network to cybersecurity threats.

Example of compliance: An employee **follows IT security training**, recognizing and reporting a phishing attempt before any harm is done.

🚨 **Strictly prohibited IT practices:**

- Using **personal USB drives or external storage** to transfer company data without IT approval.
- **Bypassing security controls** or attempting to hack into restricted areas of company systems.
- **Sharing company credentials** with unauthorized individuals.

4.3 Intellectual Property (IP) & Confidential Information

Employees must **respect and protect intellectual property** belonging to Live Now Technology SLU, as well as external organizations, partners, and competitors.

📜 **Types of Intellectual Property (IP) Covered:**

- **Trademarks & Branding –** Employees may not alter or misuse company logos, branding elements, or official documents without authorization.
- **Copyrighted Materials** – Employees must **not reproduce, distribute, or use copyrighted materials** (e.g., software, images, documents) without permission.

- **Patents & Proprietary Technology –** Employees must safeguard company innovations, patents, and proprietary technologies from unauthorized disclosure.

⚠ **Example of an IP violation:** An employee **shares proprietary software code with a competitor**, which constitutes a serious breach of intellectual property rights.

Example of compliance: An employee properly **cites external research** when using third-party materials in presentations or reports.

🚨 **Strictly prohibited activities:**

- Downloading and using **pirated software** on company devices.
- Copying or sharing **confidential project files** with **unauthorized third parties**.
- **Using company trademarks** for **personal or non-business-related** projects without approval.

📌 **Best Practices for Protecting IP:**

- Always check **licensing agreements** before using third-party materials.
- Store **sensitive files in company-approved secure locations** (e.g., encrypted cloud storage).
- **Label confidential documents appropriately** to prevent unintentional sharing.

4.4 Sustainability & Environmental Responsibility

At **Live Now Technology SLU**, we are committed to **reducing our environmental impact** and **promoting sustainability** in all aspects of our operations. Employees are encouraged to **adopt eco-friendly practices** and help the company implement **green initiatives**.

🌱 **Key Sustainability Practices:**

1. **Energy Conservation:**
   - Turn off **computers, lights, and office equipment** when not in use.
   - Use energy-efficient devices and encourage the use of **low-power mode** settings.
2. **Paper & Resource Reduction:**
   - Use **digital documentation instead of printing** whenever possible.
   - Print **double-sided** and use recycled paper when printing is necessary.
3. **Waste Management & Recycling:**
   - Employees must separate **recyclable waste** (e.g., paper, plastic, e-waste) properly.
   - Reduce **single-use plastics** by using reusable water bottles and cups.

4. **Sustainable Travel & Commuting:**
   - Employees are encouraged to **use public transportation, carpool, or remote work** options to reduce carbon footprints.
   - If traveling for work, select **eco-friendly accommodations and transportation options** where possible.

Example of a sustainable practice: Employees **use cloud storage and digital collaboration tools** instead of printing physical documents for meetings.

🚨 **Example of environmental negligence:** An employee **leaves multiple devices running overnight unnecessarily**, wasting electricity.

📌 **Company Sustainability Commitment:**
Live Now Technology SLU will:

- Regularly assess **carbon footprint** and reduce emissions where possible.
- Implement **green IT policies**, including energy-efficient data centers and sustainable procurement.
- Educate employees on **corporate social responsibility (CSR) and sustainability initiatives**.

4.5 Reporting Violations & Seeking Guidance

Employees who **witness or suspect misuse of company resources** should report the issue **confidentially** to:
📨 **IT Security Department** (for IT violations)
📨 **Legal & Compliance Team** (for intellectual property concerns)
📨 **Sustainability Officer** (for environmental impact concerns)

🔷 **No retaliation policy**: Employees will **not face punishment** for reporting good-faith concerns about misuse of company assets.

Conclusion

Live Now Technology SLU expects all employees to **use company resources responsibly, ethically, and efficiently** to ensure security, innovation, and sustainability. By following these guidelines, employees contribute to a **safe, productive, and environmentally friendly workplace**.

5. Reporting Violations & Whistleblower Protection

At **Live Now Technology SLU**, we are committed to maintaining the highest standards of **ethics, integrity, and transparency**. To ensure accountability and uphold our **Code of Conduct**, we provide employees with a **secure and anonymous reporting mechanism** for violations or unethical behavior.

Employees should feel empowered to **report concerns without fear of retaliation**, knowing that all reports will be **handled confidentially and investigated thoroughly**. This section details the reporting procedures, protections in place, and how investigations are conducted to maintain a **fair and responsible workplace**.

5.1 Importance of Reporting Violations

Every employee has a responsibility to **uphold ethical standards** and report any behavior that **violates company policies, laws, or ethical guidelines**. Prompt reporting of concerns helps **prevent misconduct from escalating** and protects the company, employees, and stakeholders.

🔍 **Types of Violations That Should Be Reported:**
✔ **Fraud, corruption, or financial misconduct –** Unauthorized use of company funds, falsification of records, or bribery.
✔ **Harassment or discrimination –** Any form of bullying, racism, sexual harassment, or unfair treatment.
✔ **Conflicts of interest –** Employees engaging in business activities that conflict with company interests.
✔ **Breach of confidentiality –** Unauthorized sharing of sensitive company information.
✔ **Cybersecurity threats & IT misuse –** Unauthorized access, hacking, or intentional security breaches.
✔ **Workplace safety violations –** Failing to adhere to **health & safety regulations**, endangering colleagues.
✔ **Environmental non-compliance –** Violations of sustainability policies or improper waste disposal.

🚨 **Example of misconduct:** A manager **pressures an employee to manipulate financial records** for personal gain.

Example of compliance: An employee reports **suspicious financial transactions** they discovered in an audit.

5.2 Reporting Mechanisms

Employees can **report violations securely and confidentially** through multiple channels:

📨 **Internal Employee Communication Channel (Anonymous Reporting Mechanism)**

- Employees can submit reports **anonymously** through an encrypted **whistleblower portal**.
- This channel is monitored by **compliance officers and an independent ethics committee** to ensure fair handling of all reports.

📞 **Direct Reporting to HR or Compliance Department**

- Employees may report concerns **directly to the HR or Legal & Compliance teams** if they prefer to disclose their identity.

📌 **Anonymous Reporting Policy:**

- Employees are **not required to reveal their identity** when submitting a report.
- All reports are treated with **the highest level of confidentiality** to protect the whistleblower's privacy.
- **Anonymous reports will be taken as seriously** as identified reports and fully investigated.

⚠ **Important: False accusations** or reports made in **bad faith** (e.g., for personal revenge or misleading information) may result in **disciplinary action**.

5.3 Non-Retaliation Policy

At **Live Now Technology SLU**, we maintain a **strict non-retaliation policy** to **protect employees** who report concerns in good faith. **No employee should fear punishment, demotion, or dismissal** for raising legitimate concerns about violations.

🔹 **Whistleblower Protections Include:**
✔ **Job Security:** Employees **cannot be fired, demoted, or penalized** for reporting concerns.
✔ **Confidentiality:** Identities will be **kept anonymous and protected** unless the employee chooses otherwise.
✔ **Protection from Workplace Retaliation:** No one can **harass, isolate, or intimidate** an employee for speaking up.

🚨 **Example of retaliation (strictly prohibited):** A manager **reduces an employee's workload and excludes them from meetings** after they report unethical conduct.

Example of compliance: A company **promotes a culture of transparency**, ensuring that whistleblowers feel safe and heard.

5.4 Investigation Process

All reports will be **investigated promptly, impartially, and thoroughly** to ensure fairness and accountability.

🔍 **How Investigations Are Conducted:**

1️⃣ **Acknowledgment of Report:**

- The **whistleblower receives confirmation** that their report has been submitted.

2️⃣ **Initial Review:**

- The Compliance Department **evaluates the severity of the claim** and determines whether a full investigation is needed.

3️⃣ **Investigation by the Ethics Committee:**

- A team of **independent investigators** will conduct interviews, collect evidence, and analyze reports.
- Employees involved will be **treated fairly** and given an opportunity to present their side.

4️⃣ **Resolution & Corrective Actions:**

- If misconduct is confirmed, **appropriate disciplinary actions** (warnings, suspensions, or legal action) will be taken.
- If needed, **company policies may be updated** to prevent future violations.

5️⃣ **Whistleblower Follow-Up:**

- Employees who submitted reports will be **updated on the outcome** while maintaining confidentiality.

📌 **Strict Confidentiality:** The identity of the whistleblower **will never be disclosed** without their consent.

🚨 **Example of a fair investigation:** An HR team **reviews evidence and interviews employees** before making a decision about a reported workplace harassment case.

5.5 Encouraging a Speak-Up Culture

At **Live Now Technology SLU**, we believe that fostering a **speak-up culture** leads to a **stronger, more ethical, and transparent** workplace. Employees are encouraged to:

✓ **Report concerns early** to prevent small issues from escalating.
✓ **Support colleagues** who speak up about misconduct.
✓ **Trust that the company will handle reports fairly and confidentially**.

Leaders & managers must:

- Promote **open communication** and encourage employees to report concerns.
- Never dismiss or **retaliate against whistleblowers**.
- Ensure all team members understand **reporting procedures and protection policies**.

Conclusion

Live Now Technology SLU is committed to **protecting employees, ensuring ethical business practices, and maintaining a fair and respectful workplace**. We encourage all employees to **report violations** and help us uphold our values of **transparency, integrity, and accountability**.

6. Disciplinary Actions

At **Live Now Technology SLU**, we are committed to **upholding the highest standards of ethics, integrity, and professionalism** in the workplace. Compliance with our **Code of Conduct** is **mandatory for all employees**, and violations will not be taken lightly.

This section outlines the **procedures for handling misconduct**, the range of **disciplinary actions that may be enforced**, and the **fair and transparent process** for addressing violations. Our goal is to ensure that all employees understand the **consequences of non-compliance** and that disciplinary actions are applied **consistently and justly**.

6.1 Purpose of Disciplinary Actions

Disciplinary measures are **not intended as punishment**, but rather as a means to:

✔ **Uphold company values and ethical standards.**
✔ **Ensure compliance with legal and regulatory requirements.**
✔ **Maintain a professional and respectful workplace.**
✔ **Protect the company, employees, clients, and stakeholders from harm.**
✔ **Encourage corrective behavior and prevent repeat violations.**

A **fair and structured disciplinary process** ensures that all employees are **held accountable** for their actions while also being given an opportunity to **improve and correct behavior when possible**.

🚨 **Example of a minor violation:** An employee repeatedly arrives late to meetings without valid justification.
🚨 **Example of a severe violation:** An employee **steals confidential client data** and sells it to competitors.

6.2 Types of Violations That May Lead to Disciplinary Actions

🔍 Disciplinary actions may be taken for, but are not limited to, the following violations:

6.2.1 Workplace Misconduct & Policy Violations

- Harassment, bullying, discrimination, or any form of **abusive behavior**.

- Breach of **workplace safety protocols**, endangering employees or company property.
- Use of **offensive, inappropriate, or discriminatory language** in the workplace.

6.2.2 Breach of Confidentiality & Data Protection

- Unauthorized **disclosure of company-sensitive information**.
- Mishandling of **confidential data**, including client or employee records.
- **Failure to comply with cybersecurity policies**, leading to potential data breaches.

6.2.3 Fraud, Corruption & Financial Misconduct

- Engaging in **bribery, embezzlement, falsification of records, or financial fraud**.
- **Misuse of company funds or property** for personal gain.
- **Submitting false expense claims or forging documents**.

6.2.4 Misuse of Company Resources & IT Systems

- **Unauthorized access to systems, hacking, or altering company data**.
- **Using company assets for illegal or unethical purposes**.
- **Violation of intellectual property laws**, including unauthorized software use.

6.2.5 Non-Compliance with Legal & Regulatory Requirements

- **Failure to comply with GDPR**, cybersecurity laws, or industry regulations.
- **Neglecting occupational health and safety standards**, creating unsafe work environments.
- **Engaging in unethical business practices** that could result in legal liabilities.

6.3 Types of Disciplinary Actions

🔹 Disciplinary actions will be **proportionate to the severity of the violation** and will take into account **intent, impact, and recurrence**. Actions may include:

6.3.1 Informal Corrective Measures (For Minor Violations)

Verbal Warning: A private conversation with a supervisor to address minor issues.
Coaching & Additional Training: The employee may be required to complete a training program to improve behavior or knowledge gaps.

📝 **Example:** If an employee **inadvertently violates a company policy**, they may receive additional guidance rather than immediate disciplinary action.

6.3.2 Formal Disciplinary Actions

🚨 **Written Warning:** A formal document stating the nature of the violation, corrective actions required, and potential consequences of further misconduct.
🚨 **Performance Improvement Plan (PIP):** If the issue is performance-related, the employee may be placed on a structured **improvement program** with clear goals and deadlines.

📝 **Example:** An employee who **continuously disregards deadlines and underperforms despite multiple reminders** may be placed on a **Performance Improvement Plan** before further action is taken.

6.3.3 Serious Disciplinary Actions (For Severe or Repeated Violations)

⛔ **Suspension Without Pay:** For major violations, the employee may be temporarily suspended while an investigation is conducted.
⛔ **Demotion or Reassignment:** If appropriate, an employee may be moved to a different role with **fewer responsibilities**.

📝 **Example:** If an employee **repeatedly fails to comply with security policies** and exposes sensitive data, they may be **reassigned to a non-sensitive role** or placed on suspension.

6.3.4 Termination of Employment

❌ **Immediate Dismissal for Gross Misconduct:** Employees may be terminated without prior warning if they engage in:

- **Theft, fraud, or intentional harm to company reputation.**
- **Violent or criminal behavior within the workplace.**
- **Severe ethical violations, such as corruption or discrimination.**

📝 **Example:** If an employee **commits an act of workplace violence or engages in serious fraudulent activity**, they may be immediately terminated.

6.3.5 Legal Action & Criminal Charges

⚖ **Legal Proceedings:** In cases of criminal conduct (e.g., fraud, cybercrime, data theft), the company may pursue **legal action** against the employee.

⚖ **Civil or Criminal Liability:** Employees found guilty of serious misconduct may face **lawsuits, fines, or prosecution**.

📝 **Example:** If an employee **steals intellectual property and sells it to competitors**, legal action may be pursued.

6.4 Disciplinary Process & Employee Rights

All disciplinary actions will be **handled with fairness, confidentiality, and due process**. Employees **have the right** to:

✓ **Receive a clear explanation** of the alleged violation.
✓ **Provide their side of the story** before disciplinary actions are taken.
✓ **Have a representative (HR or legal counsel) present** during hearings.
✓ **Appeal against decisions** if they believe the disciplinary action was unfair.

6.5 Appeals & Review Process

Employees who **disagree with disciplinary actions** may submit an appeal within **10 business days**. The **HR Department and Ethics Committee** will conduct a **secondary review** before making a final decision.

✓ **Appeals must be submitted in writing**, detailing why the disciplinary action was unjustified.
✓ **Further investigation may be conducted**, including interviews and evidence review.
✓ **Final decisions will be communicated in writing** within a specified timeframe.

6.6 Preventive Measures & Company Commitment

At **Live Now Technology SLU**, our focus is on **prevention rather than punishment**. We believe in:

✓ **Ongoing training** to help employees understand company policies.
✓ **Clear communication of expectations** to avoid misunderstandings.
✓ **Encouraging employees to seek clarification** before violating any rules.
✓ **Maintaining a fair and objective disciplinary process**.

Conclusion

Disciplinary actions exist to **protect employees, clients, and company integrity**. By understanding and respecting company policies, employees contribute to a **fair, safe, and ethical workplace**.

Acknowledgment

At **Live Now Technology SLU**, we take our **Code of Conduct** seriously. This document outlines the fundamental values, principles, and policies that guide our actions, interactions, and responsibilities within the company and towards our stakeholders.

All **employees, contractors, and business partners** are expected to **read, understand, and fully comply** with the provisions outlined in this Code. By signing the acknowledgment statement, individuals confirm their commitment to ethical and responsible conduct, fostering a professional and respectful work environment.

1. Who Must Acknowledge This Code?

📌 **All Employees –** Every employee, regardless of position, seniority, or department, must adhere to the policies outlined in this Code.
📌 **Contractors & Consultants** – Third-party professionals working with or on behalf of the company must also comply with these guidelines.
📌 **Business Partners & Vendors –** Any organization or individual engaging in business activities with **Live Now Technology SLU** is required to uphold similar ethical standards.

Failure to acknowledge or comply with this Code may result in disciplinary actions, including contract termination, legal repercussions, or disqualification from future collaborations.

2. Employee & Contractor Responsibilities

Read & Understand – All employees and associated personnel must carefully review the entire Code of Conduct.
Comply with the Policies – Individuals are expected to apply these principles in daily work activities and decision-making processes.
Seek Clarification When Needed – If any section of the Code is unclear, employees should consult their manager or the **HR & Compliance Department** for guidance.
Report Ethical Concerns – Employees must proactively report violations, unethical behavior, or misconduct through the **Internal Employee Communication Channel (Anonymous Reporting Mechanism)**.

🔹 **Example:** If an employee notices a security breach but does not report it, this could lead to serious consequences. Ethical responsibility includes taking **proactive steps** to address potential risks.

3. Business Partners & Vendor Commitment

Live Now Technology SLU requires that all external parties—including vendors, suppliers, and partners—follow the ethical principles outlined in this Code when conducting business with or on behalf of the company.

🔍 **Key Expectations from Business Partners:**

- **Integrity in Transactions:** All agreements, contracts, and financial dealings must be transparent and free from corruption or fraudulent practices.
- **Data Protection & Confidentiality:** Any access to company or customer data must be handled with the utmost security and in compliance with **GDPR and cybersecurity best practices**.
- **Workplace Ethics & Compliance:** Business partners must not engage in discrimination, harassment, forced labor, or any unethical business practices.

Any third-party found violating this Code may face **contract termination, legal repercussions, and loss of business opportunities** with our company.

4. Commitment to Continuous Ethical Improvement

At **Live Now Technology SLU**, we continuously **review, update, and improve** our Code of Conduct to:

✓ Align with **industry best practices** and evolving regulations.
✓ Address new challenges in **data protection, cybersecurity, and workplace ethics**.
✓ Reinforce a **culture of integrity and ethical responsibility**.

Employees, contractors, and business partners will be **notified of any significant changes** to this Code, and updated acknowledgments may be required when major revisions occur.

Information security policy

The **Information Security Policy** is a critical document that outlines the principles, rules, and procedures that **Live Now Technology SLU** follows to **protect sensitive data, ensure compliance with regulations, and mitigate security risks**.

1. Introduction & Purpose

1.1 Introduction

At **Live Now Technology SLU**, information security is a fundamental pillar of our operations. As a company specializing in **data processing, system engineering, and scientific software development**, we handle **sensitive corporate, client, and personal data** that must be **protected against unauthorized access, disclosure, alteration, or destruction**.

The increasing sophistication of cyber threats, regulatory requirements, and our commitment to **data privacy** necessitate a structured and proactive **information security framework**. This policy outlines the principles, rules, and responsibilities that govern **how we protect digital assets, mitigate risks, and ensure business continuity**.

1.2 Purpose of the Policy

The objective of this Information Security Policy is to:
Protect the confidentiality, integrity, and availability (CIA) of company and client data.
Ensure compliance with applicable regulations, including **GDPR, ISO/IEC 27001, and national cybersecurity laws**.
Prevent data breaches, unauthorized access, and cyber threats by implementing strict security controls.
Educate employees, contractors, and third parties on their security responsibilities.
Establish a framework for risk management, incident response, and business continuity.
Maintain trust with clients, partners, and stakeholders by demonstrating a strong security posture.

By adhering to this policy, **Live Now Technology SLU** aims to safeguard its business, customers, and employees from **data loss, cyberattacks, and reputational damage**.

2. Scope & Applicability

2.1 Scope

This **Information Security Policy** applies to all **systems, networks, devices, data, and personnel** within **Live Now Technology SLU**. It defines security principles for **protecting digital assets** and ensuring the confidentiality, integrity, and availability of **company and client information**.

It covers, but is not limited to:

Company-owned IT infrastructure (servers, databases, cloud environments, and workstations).

Network security (firewalls, VPNs, access controls, and secure communication protocols).

Company and client data (electronic documents, databases, email communications, and backups).

Software development and deployment security (coding standards, vulnerability testing, and version control).

User authentication and access control (identity management, password policies, and multi-factor authentication).

Third-party service providers and contractors (outsourced IT services, cloud providers, and business partners).

Physical security measures (office security, restricted areas, and controlled access).

Incident response and disaster recovery plans (business continuity and data restoration protocols).

2.2 Applicability

This policy applies to **all employees, contractors, and third parties** who interact with company systems and data. It is mandatory for:

- **Full-time and part-time employees**, including remote workers.
- **Contractors, freelancers, and consultants** with access to company data or IT systems.
- **Third-party vendors, suppliers, and partners** handling or storing company data.
- **Interns, trainees, and temporary staff** using company devices or software.

All personnel must:

📌 **Understand and comply** with security policies, procedures, and guidelines.

📌 **Report any security breaches, threats, or incidents** immediately.

📌 **Follow access control policies** and never share credentials or sensitive data.

📌 **Adhere to best practices for handling data, devices, and online communications**.

Failure to comply with this policy may result in **disciplinary actions, contract termination, or legal consequences**.

3. Information Security Principles

This section outlines the **core security principles** that govern how **Live Now Technology SLU** protects its data, IT assets, and business operations. These principles ensure compliance with **European data protection laws (GDPR), industry standards, and best practices** for securing sensitive information.

3.1 Confidentiality

Protecting sensitive information from unauthorized access or disclosure is a top priority.

Data Classification & Access Control

- All data is classified as **Public, Internal, Confidential, or Restricted** based on sensitivity.
- Access to **Confidential and Restricted data** is granted on a **need-to-know basis** using role-based access controls (RBAC).
- **Multi-Factor Authentication (MFA)** is enforced for accessing sensitive systems.
- Data access is reviewed periodically to **remove unnecessary privileges**.

Encryption Standards

- All confidential data is **encrypted at rest and in transit** using AES-256 or equivalent.
- Secure communication channels (e.g., **SSL/TLS, VPNs**) are required for remote access.
- Sensitive files must be stored in **encrypted databases or secure cloud storage**.

Data Sharing & Transmission

- Employees must use **company-approved tools (e.g., encrypted email, VPN, secure file transfer services)** for data sharing.
- **Personal email accounts, USB devices, and unauthorized cloud storage** are strictly prohibited for handling company data.

3.2 Integrity

Ensuring data and systems are **accurate, consistent, and tamper-proof**.

Version Control & Change Management

- Software updates and system changes must follow a **controlled process**, with approvals and version tracking.
- Logs must be maintained for **all modifications to critical systems and applications**.
- Automated integrity checks ensure **data consistency and prevent unauthorized changes**.

Protection Against Unauthorized Modifications

- Access to **critical systems, databases, and source code** is strictly controlled.
- Digital signatures and hash algorithms are used to **verify file authenticity**.
- Anomaly detection systems **alert security teams** to unusual system changes.

Data Validation & Error Handling

- Input validation and sanitization techniques must be applied to prevent **injection attacks**.
- Automated testing is required for **data consistency checks** before production deployment.
- Backups must undergo **regular integrity testing** to ensure recoverability.

3.3 Availability

Ensuring systems, services, and data are accessible **when needed** without disruption.

Business Continuity & Disaster Recovery

- Critical systems have **redundancy and failover mechanisms** to prevent downtime.
- **Regular backups** are maintained in secure locations, with **automated recovery testing**.
- A **Business Continuity Plan (BCP)** outlines procedures to resume operations after disruptions.

Cyber Resilience & Threat Mitigation

- DDoS protection, load balancing, and **real-time monitoring** help prevent service disruptions.
- Network and system health **must be continuously monitored for performance and security issues**.

- Incident response teams **must be on-call for immediate threat mitigation**.

Remote Access & System Uptime

- Remote access is **restricted to company-approved VPNs and devices**.
- Cloud services and infrastructure providers must meet **99.9% uptime SLAs**.
- Employees must report **any system failures, connectivity issues, or slow performance immediately**.

4. Access Control & User Authentication

Access control is a **fundamental pillar** of information security at **Live Now Technology SLU**. It ensures that **only authorized individuals** can access company data, systems, and resources while **preventing unauthorized access, data breaches, and security threats**.

4.1 User Authentication

Proper authentication mechanisms protect **systems, networks, and sensitive data** from unauthorized access.

Multi-Factor Authentication (MFA)

- All employees, contractors, and third-party vendors must use **MFA** when accessing company systems.
- MFA methods include **password + OTP (One-Time Password), biometric authentication, or security tokens**.
- Admin accounts must use **hardware-based authentication** (e.g., YubiKeys, smart cards).

Password Security & Management

- Employees must create **strong, unique passwords** using at least:
    - **12+ characters** (including uppercase, lowercase, numbers, and symbols).
    - **No dictionary words or common phrases**.
- Passwords must be **changed every 90 days** and should never be reused.
- The company enforces a **password manager policy**, requiring employees to store credentials in an **approved password manager**.
- **Account lockout policy**: After **five failed login attempts**, accounts will be locked for **15 minutes**.

Single Sign-On (SSO) & Federated Identity

- Employees authenticate using **SSO (Single Sign-On)** for all integrated corporate services.
- **Federated identity management** (via Azure AD, Okta, or Google Workspace) allows **secure, centralized authentication** across different platforms.

4.2 Access Control Policies

Role-based and **least privilege access** ensures employees **only have access to what they need**.

Role-Based Access Control (RBAC)

- Access is granted based on **job role and responsibilities** (e.g., IT Admins, Finance, HR).
- Employees receive **minimum necessary permissions** to perform their job.
- Higher privilege access (e.g., system admin rights) is **strictly controlled and monitored**.

Principle of Least Privilege (PoLP)

- Users and systems are granted **only the minimum level of access necessary** to perform their functions.
- **Temporary or elevated access** must be formally requested, justified, and **time-restricted**.
- Sensitive data and administrative actions are **restricted to authorized personnel only**.

Access Reviews & Revocation

- User access permissions are **reviewed quarterly** to detect and remove **inactive or unnecessary accounts**.
- Employees leaving the company have **all access revoked immediately** on their last working day.
- Dormant accounts (inactive for **90 days**) are automatically **disabled and flagged for review**.

4.3 Third-Party & Vendor Access

External parties **must follow strict security policies** when accessing company resources.

Vendor Risk Management

- Third-party vendors undergo **a security assessment** before being granted access.
- Contracts include **clear security clauses**, ensuring vendors **follow our security policies**.
- Vendor access is **restricted to dedicated environments** (never on production systems).

Secure Remote Access

- External users must **authenticate via VPN** and **use MFA** before accessing company resources.
- Remote access sessions are **monitored, logged, and reviewed** for security violations.
- Vendors must **disconnect immediately after completing assigned tasks**.

Data Sharing Controls

- Third-party access to confidential data **requires management approval**.
- Sensitive data **must be anonymized or masked** before being shared externally.
- All data transfers occur via **encrypted channels (TLS 1.2+, SFTP, or secure APIs)**.

4.4 Logging & Monitoring of Access

To detect unauthorized activities, all **authentication events and access attempts** are logged and reviewed.

Real-Time Monitoring & Alerts

- All login attempts, failed authentication events, and privilege escalations are **logged and analyzed**.
- Anomalies (e.g., unusual login locations, repeated access failures) trigger **immediate security alerts**.

Audit Trails & Compliance Logs

- Detailed access logs are stored **for at least 12 months** for audit and compliance purposes.
- Regular security audits ensure that **access control policies remain effective**.

Incident Response for Unauthorized Access

- If unauthorized access is detected, the **account is suspended immediately**, and an investigation is launched.
- Employees **must report** any suspicious access attempts to the **IT Security Team**.

5. Data Handling & Encryption

Data security is at the core of **Live Now Technology SLU's** information security strategy. Ensuring that data is **properly handled, stored, transmitted, and disposed of** is essential to protecting company assets, intellectual property, and customer information.

5.1 Data Classification & Sensitivity Levels

All company data is categorized based on **sensitivity and confidentiality requirements** to apply the appropriate security controls.

Classification Levels:

1. **Public** – Data that can be freely shared without risk (e.g., website content, job postings).

2. **Internal Use Only** – Non-sensitive business information, accessible to employees but not the public (e.g., internal documentation, training materials).

3. **Confidential** – Data that requires protection due to **business, legal, or regulatory reasons** (e.g., contracts, HR records, financial information).

4. **Restricted / Highly Confidential –** The most sensitive information, requiring **strict access control and encryption** (e.g., trade secrets, personal data, security credentials).

Access Restrictions:

- **Public Data** can be freely shared.

- **Internal Data** is restricted to employees only.

- **Confidential Data** is shared on a **need-to-know basis**, requiring managerial approval.
- **Highly Confidential Data** requires **multi-factor authentication, encryption, and audit logging**.

5.2 Data Encryption & Secure Storage

Encryption Policies:

- **All sensitive data** must be encrypted **at rest and in transit** using industry-standard encryption algorithms.
- **Encryption at Rest:**
  - Company databases use **AES-256 encryption**.
  - Workstations, laptops, and mobile devices **must have full-disk encryption enabled**.
- **Encryption in Transit:**
  - All data transfers use **TLS 1.2+ encryption** to prevent interception.
  - Internal and external emails containing sensitive information must be **encrypted using PGP or S/MIME**.

Secure Storage Best Practices:

- Data **must not be stored on personal devices** or unauthorized cloud storage services.
- Confidential data is stored in **company-approved encrypted repositories** (e.g., **OneDrive for Business, Google Workspace, AWS S3 with encryption**).
- Paper documents containing confidential data must be **locked in secure cabinets**.

5.3 Data Retention & Disposal

To comply with **legal, regulatory, and operational** requirements, we implement **strict data retention and disposal policies**.

Retention Periods:

- Employee records: **5 years** after termination.
- Financial records: **7 years** as per tax regulations.
- Customer and project data: **As per contractual agreements**.
- Backups: **Regularly reviewed and purged based on business needs**.

Secure Data Disposal:

- **Digital Data:** Must be securely erased using **military-grade wiping tools** (e.g., **DoD 5220.22-M standard**).
- **Physical Documents:** Must be **shredded and securely disposed of**.
- **Hardware Disposal:** Storage devices must be **physically destroyed or securely wiped** before disposal.

6. Network Security & Infrastructure Protection

Protecting our network infrastructure is fundamental to **Live Now Technology SLU's** commitment to cybersecurity. A **multi-layered defense approach** ensures the integrity, availability, and confidentiality of company systems, preventing **unauthorized access, cyber threats, and data breaches**.

6.1 Perimeter Security & Firewalls

We implement **multiple security layers** at the **perimeter, network, and endpoint levels** to detect and prevent external threats.

Firewall & Intrusion Prevention Systems (IPS):

- All external connections pass through **enterprise-grade firewalls** configured with **deep packet inspection (DPI)**.

- **IPS and IDS (Intrusion Detection Systems)** are deployed to **detect and block malicious traffic**.

- Regular **security audits and rule updates** ensure **firewall policies** are aligned with emerging threats.

Geo-Blocking & Access Restrictions:

- Traffic from high-risk countries and known malicious IP addresses is **automatically blocked**.

- **Strict access policies** apply to remote connections, requiring **multi-factor authentication (MFA)**.

6.2 Internal Network Segmentation & Zero Trust Security

We follow a **Zero Trust security model**, which **eliminates the assumption of trust** within the network and enforces strict authentication and verification for every access request.

Network Segmentation Strategy:

- Internal networks are **segmented into isolated zones** to **limit attack spread** in case of a breach.

- **Sensitive data and critical services** (e.g., finance, HR, and R&D servers) reside in **separate VLANs** with **restricted access**.

- Employees are granted access **only to the resources required for their job roles** (**Principle of Least Privilege**).

Zero Trust Security Model:

- **Verify identity before granting access** – all users must pass authentication checks.

- **Micro-segmentation ensures** that different departments and functions **do not share the same network space**.

- **Real-time monitoring** identifies abnormal access patterns and potential **insider threats**.

6.3 Secure Wi-Fi & Remote Access Policy

Ensuring secure access to **corporate systems** from both internal Wi-Fi and remote environments is critical for preventing unauthorized intrusions.

Corporate Wi-Fi Security:

- **WPA3 encryption** is enforced on all company Wi-Fi networks.
- Guest networks are **completely isolated** from corporate infrastructure.
- **MAC address filtering** restricts access to **pre-approved devices only**.

Remote Access via VPN:

- Remote employees **must use the company-approved VPN** to access internal systems.
- **Split tunneling is disabled** to ensure all traffic flows through the VPN.
- VPN access requires **multi-factor authentication (MFA)**.

6.4 Endpoint Security & Device Management

To prevent endpoint-level attacks such as **ransomware, malware, and phishing**, we enforce **strict device security policies**.

Mandatory Security Software:

- All company devices must have **next-gen antivirus (NGAV) and endpoint detection & response (EDR)** solutions.
- **Automatic patching** ensures software and OS vulnerabilities are quickly addressed.

Device Hardening Policies:

- **USB ports are restricted** to prevent unauthorized data transfer.
- **Admin privileges are limited** to prevent unauthorized software installations.
- **Full-disk encryption** is required on all **laptops, desktops, and mobile devices**.

6.5 Secure Cloud & Data Center Operations

As a technology-driven company, **Live Now Technology SLU** relies on a **hybrid cloud environment**, combining **on-premise data centers** with **secure cloud services**.

Cloud Security Best Practices:

- Cloud resources are **protected with identity-based access controls (IAM)**.
- **Data is encrypted at rest and in transit** with AES-256 and TLS 1.2+.
- **Regular cloud security audits** identify misconfigurations and vulnerabilities.

On-Premise Security Standards:

- Data centers require **biometric authentication** and **24/7 monitoring**.
- **Disaster recovery plans** ensure business continuity in case of failure.
- **Access logs are continuously reviewed** to prevent unauthorized entry.

6.6 Continuous Network Monitoring & Threat Intelligence

To proactively detect and mitigate threats, we implement **real-time monitoring and threat intelligence**.

Security Information & Event Management (SIEM):

- Logs from firewalls, servers, and endpoints are **centralized** in a **SIEM system**.
- **Machine learning algorithms** identify anomalies and suspicious behavior.

Threat Intelligence & Automated Response:

- Threat intelligence feeds provide **real-time updates** on **cyber threats and indicators of compromise (IOCs)**.
- Automated **threat response mechanisms** isolate infected systems before an attack spreads.

6.7 Compliance with Industry Security Standards

Live Now Technology SLU adheres to **global cybersecurity frameworks** to maintain the highest security standards.

Regulatory & Compliance Adherence:

- **ISO 27001** – Information security management system (ISMS).
- **NIST Cybersecurity Framework –** Risk-based cybersecurity best practices.
- **GDPR & Data Privacy Regulations –** Ensuring user data protection and compliance.

Regular Security Audits & Penetration Testing:

- Annual **third-party penetration tests** identify vulnerabilities.
- Internal **security audits ensure compliance** with evolving cyber threats.

7. Incident Response & Breach Management

A **proactive and well-defined incident response strategy** is essential to mitigate the impact of security breaches and cyber threats. **Live Now Technology SLU** follows a **structured incident response framework** to ensure that all security events are **quickly identified, investigated, contained, and resolved** while maintaining compliance with **legal and regulatory requirements**.

7.1 Incident Classification & Identification

Security incidents vary in scope and severity. **Live Now Technology SLU** categorizes incidents based on potential impact and follows a **prioritization matrix**:

Incident Severity Levels:

- **Low (Minor Events)** – Unauthorized login attempts, minor phishing emails, or isolated malware detections.
- **Medium (Moderate Threats)** – Compromised employee accounts, unauthorized access to non-sensitive data.
- **High (Critical Incidents)** – Data breaches, system-wide ransomware attacks, denial-of-service (DoS) attacks, or insider threats.

Early Threat Detection Mechanisms:

- **Security Information and Event Management (SIEM):** Logs and events are continuously monitored for unusual activity.
- **User & Entity Behavior Analytics (UEBA):** AI-driven anomaly detection helps **identify malicious behaviors** within the network.
- **Automated Alerting:** Suspicious activities trigger **immediate security alerts** for investigation.

7.2 Incident Reporting & Escalation Procedures

Employees and IT security personnel must **report any suspected security incident** immediately through the **Internal Security Incident Response System**.

Incident Reporting Channels:

- Employees can report security concerns via:
    - Internal security hotline 📞
    - Dedicated email 📨
    - Anonymous internal reporting system 🕵
- IT Security & Incident Response Teams (SIRT) receive real-time alerts via **automated monitoring systems**.

Escalation Levels & Responsibilities:

- **Tier 1 (IT Helpdesk & Security Team):** Initial triage and analysis of reported incidents.
- **Tier 2 (Security Operations Center - SOC):** Advanced investigation, forensic analysis, and containment efforts.
- **Tier 3 (Executive & Legal Response Team):** Crisis management, compliance assessment, legal action if required.

7.3 Containment & Remediation Strategies

Once an incident is confirmed, a rapid response is essential to prevent further damage and restore operations.

Containment Measures:

- **Isolate affected systems** immediately (e.g., disconnect infected devices from the network).
- **Block malicious IP addresses** and suspend compromised accounts.
- **Deactivate unauthorized remote access** to prevent lateral movement within the infrastructure.

Forensic Analysis & Root Cause Investigation:

- **Digital forensics experts analyze attack patterns** and determine entry points.
- **Incident logs, system snapshots, and security reports** are collected for evidence.
- **Vulnerability analysis is conducted** to prevent similar future incidents.

Eradication & Recovery:

- **Malware removal and system clean-up** through advanced antivirus and forensic tools.
- **Restoration of data from secure backups** (ensuring integrity before reintegration).

- **Patch vulnerabilities** identified during the attack and reinforce security configurations.

7.4 Communication & Stakeholder Notification

For incidents involving **data breaches or legal implications**, **Live Now Technology SLU** follows **strict notification protocols** in compliance with **GDPR, ISO 27001, and NIST**.

Internal Communication Plan:

- Security teams inform **executive leadership, compliance officers, and affected departments**.
- Regular updates are provided to **ensure transparency and coordinated efforts**.

External Notifications (GDPR Compliance):

- If personal data is exposed, affected users must be notified **within 72 hours** per **GDPR Article 33**.
- If applicable, the incident is reported to the **European Data Protection Authority (DPA)**.
- Affected clients or stakeholders receive official **incident reports** with recommended next steps.

Legal & Public Relations Handling:

- If a major security event affects **Live Now Technology SLU's reputation**, the **Public Relations (PR) team** coordinates external communication.
- Legal advisors guide **compliance with breach disclosure laws** and potential liabilities.

7.5 Post-Incident Analysis & Security Improvements

After every incident, **a full review is conducted** to strengthen security defenses and prevent recurrence.

Post-Incident Report (PIR):

- Detailed analysis of **root causes, affected systems, and attack vectors**.
- Identification of **security gaps and control weaknesses**.
- **Actionable recommendations** to improve cybersecurity posture.

Security Enhancements:

- **Patching vulnerabilities** exploited in the attack.
- **Implementing additional security measures** (e.g., stronger access controls, improved monitoring tools).
- **Employee cybersecurity training** based on lessons learned from the incident.

7.6 Compliance with International Security Standards

Live Now Technology SLU follows global security standards for **incident response management**:

- **ISO 27035 –** Information Security Incident Management
- **NIST SP 800-61 –** Computer Security Incident Handling Guide
- **GDPR Article 33 & 34 –** Personal Data Breach Notification

By adhering to these frameworks, we ensure a **robust, compliant, and effective** approach to **incident response and breach management**.

8. Security Awareness & Training Programs

A strong cybersecurity culture is one of the most effective defenses against evolving threats. **Live Now Technology SLU** is committed to building and maintaining a **high level of security awareness** among all employees, contractors, and third parties. We achieve this through **mandatory training programs, continuous education initiatives, and regular simulated exercises**.

8.1 Importance of Security Awareness

Human error is responsible for a significant percentage of security breaches worldwide. **Informed and vigilant employees** are our first line of defense against threats like phishing, social engineering, ransomware, and insider attacks.

Security awareness empowers employees to:

- Recognize suspicious activities and potential threats.
- React appropriately to security incidents.
- Protect confidential information and company assets.
- Understand legal and regulatory requirements such as **GDPR** and **ISO 27001** standards.

8.2 Mandatory Security Training for All Employees

All employees, contractors, and relevant third parties **must complete initial security training** during onboarding and **participate in ongoing annual refresher courses**.

Core Training Topics Include:

- Fundamentals of information security (CIA: Confidentiality, Integrity, Availability).
- Password security and best practices.
- Identifying and avoiding phishing and social engineering attacks.
- Protecting sensitive and personal data (GDPR compliance).
- Safe use of IT resources (workstations, mobile devices, cloud services).
- Secure remote working practices and VPN usage.
- Proper reporting procedures for security incidents or breaches.

Training Requirements:

- Training must be completed within **30 days of hire**.
- Annual security training is mandatory, with completion tracked by **HR and Compliance Departments**.
- Passing a **knowledge assessment** (minimum 80% correct answers) is required after each session.

8.3 Specialized Security Training for Key Roles

Certain roles have access to **critical systems and sensitive data** and therefore require **advanced security training**:

Additional Training for:

- **IT staff:** Network security, incident response, and vulnerability management.
- **Developers:** Secure coding practices (OWASP Top 10, code review techniques).
- **Project Managers:** Data handling regulations and third-party vendor risk management.
- **Executive Management:** Cyber risk management and regulatory compliance responsibilities.

8.4 Ongoing Awareness Initiatives

Security awareness must be **continuous, dynamic, and engaging**.

Regular Awareness Campaigns:

- Monthly **security newsletters** with real-world case studies and emerging threats.
- Posters and infographics throughout office spaces reinforcing best practices.
- Short videos highlighting simple security tips.

Simulated Phishing Tests:

- **Quarterly phishing simulations** are conducted to measure employee vigilance.

- Employees who fail simulations are required to **attend additional security coaching sessions**.

Interactive Workshops & Webinars:

- Guest cybersecurity experts deliver **bi-annual workshops** on evolving threats like ransomware, social engineering, and AI-driven attacks.

- Webinars provide convenient access to important updates and skills refreshers.

8.5 Promoting a Security-First Mindset

Beyond mandatory training, **Live Now Technology SLU** strives to **embed security into the company culture** by encouraging:

- **Proactive behavior:** Employees are urged to **report suspicious activity immediately**, even if uncertain.
- **Reward programs:** Recognizing employees who actively contribute to **improving security practices**.
- **Open communication:** Encouraging questions, clarifications, and discussions on security-related topics without fear of judgment.
- **Security champions:** Appointing volunteers in different departments to **advocate security best practices locally**.

8.6 Tracking & Compliance Monitoring

Training Records:

- Training completion is tracked and reported quarterly to senior management.

- Non-compliance triggers reminders, escalations, and, if necessary, disciplinary measures.

Continuous Improvement:

- Feedback from employees is collected to **enhance future training programs**.

- Programs are reviewed **annually** based on threat landscape changes and evolving business needs.

8.7 Alignment with Security Standards

Our security training program is aligned with leading standards and best practices, including:

- **ISO/IEC 27001 Annex A.7.2.2** — Information security awareness, education, and training.
- **NIST Special Publication 800-50** — Building an Information Technology Security Awareness and Training Program.
- **GDPR Article 32** — Security of processing and employee awareness requirements.

9. Compliance with Legal & Regulatory Standards

Compliance with legal and regulatory standards is a **cornerstone** of **Live Now Technology SLU's** information security strategy. As an organization operating in Europe and handling sensitive data, we are committed to **strict adherence** to applicable **laws, regulations, and international standards** that govern data protection, privacy, and information security.

9.1 Regulatory Frameworks and Compliance Obligations

General Data Protection Regulation (GDPR)

- **Scope:** Applies to all organizations processing personal data of individuals within the European Economic Area (EEA).
- **Key Compliance Areas:**
  - Lawful, fair, and transparent data processing.
  - Data minimization and purpose limitation.
  - Ensuring data accuracy and storage limitation.

  - Securing personal data against unauthorized access, alteration, or loss.
  - Upholding the rights of data subjects (access, rectification, erasure, portability).
  - Notification of personal data breaches within **72 hours** to supervisory authorities.

ISO/IEC 27001 — Information Security Management Systems (ISMS)

- **Scope:** International standard providing a systematic approach to managing sensitive company information.
- **Key Compliance Areas:**
  - Establishing a risk management framework for information security.
  - Implementing security controls based on ISO 27002 best practices.
  - Regular internal audits and external certifications (where applicable).
  - Continuous improvement through the PDCA cycle (Plan, Do, Check, Act).

NIS2 Directive (Upcoming Compliance Focus for EU Entities)

- **Scope:** Network and Information Systems Directive affecting essential and important entities across the EU.
- **Key Compliance Areas:**
  - Strengthening cybersecurity resilience across sectors.
  - Mandatory incident reporting within **24 hours**.
  - Higher scrutiny of third-party risks and supply chains.

Other Applicable Regulations:

- **Spanish LOPDGDD (Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales):** National implementation complementing GDPR.

- **ePrivacy Directive (Cookie Law):** Compliance with electronic communications privacy (cookies, marketing emails, etc.).
- **Employment Law:** Protection of employee personal data under labor regulations.

9.2 Measures Implemented for Regulatory Compliance

Data Protection Officer (DPO) Role:

- A **DPO** (internal or external) oversees data protection strategies and ensures compliance with GDPR and local data privacy laws.
- The DPO acts as the **primary point of contact** with regulatory authorities and data subjects.

Data Processing Agreements (DPAs):

- Mandatory DPAs are signed with all **third-party processors** handling personal data.
- DPAs ensure compliance with GDPR Article 28 requirements (e.g., subprocessing controls, security measures, audits).

Privacy by Design and Default:

- New systems, services, and processes are developed with **data protection embedded** from the outset.
- Only the **necessary amount of personal data** is collected and processed for each purpose.

Data Protection Impact Assessments (DPIAs):

- Conducted for high-risk processing activities involving sensitive data, large-scale profiling, or new technologies.
- DPIAs assess potential impacts on privacy and propose mitigation measures before deployment.

Secure International Data Transfers:

- Data transfers outside the EU/EEA are conducted under:
    - **Standard Contractual Clauses (SCCs)** approved by the European Commission.
    - **Adequacy decisions** where applicable.
    - **Appropriate supplementary measures** if needed.

Incident Response & Breach Notification:

- Incident response plans ensure that personal data breaches are reported promptly to supervisory authorities and, where necessary, to affected individuals.

9.3 Monitoring, Auditing, and Documentation

Internal Compliance Audits:

- Annual audits assess the effectiveness of security measures, regulatory compliance, and risk management practices.
- Findings are documented and corrective actions are implemented.

Record Keeping:

- A **Register of Processing Activities** (ROPA) is maintained as per GDPR Article 30.
- Security incidents, data breach reports, and DPIAs are thoroughly documented.

Vendor Monitoring:

- Regular reviews of third-party vendors' compliance with contractual security and privacy obligations.
- Third-party security questionnaires and on-site audits (for high-risk vendors).

9.4 Non-Compliance Consequences

Failure to comply with legal and regulatory standards may result in:

- Administrative fines (e.g., GDPR fines up to **€20 million** or **4% of annual global turnover**, whichever is higher).
- Reputational damage and loss of customer trust.
- Legal actions, civil penalties, and regulatory sanctions.
- Termination of vendor relationships for non-compliant third parties.

9.5 Commitment to Continuous Compliance

Live Now Technology SLU commits to:
Staying informed about evolving cybersecurity and data protection regulations.
Updating security and privacy policies proactively.
Educating employees on their legal obligations.
Engaging with regulators transparently and cooperatively.

10. Policy Review & Updates

To ensure that our information security framework remains **effective, relevant, and compliant** with evolving threats, technologies, and regulations, **Live Now Technology SLU** is committed to a **continuous review and improvement process** for this Information Security Policy.

A static policy cannot adequately protect a dynamic organization; therefore, **regular updates, audits, and reviews** are essential to maintain **optimal security posture and regulatory compliance**.

10.1 Review Frequency

Annual Review:

- This Information Security Policy is reviewed **at least once every 12 months** to ensure it remains accurate, comprehensive, and aligned with current threats, technologies, and legal requirements.

Event-Driven Reviews:

The policy will also be reviewed and updated immediately if any of the following occur:

- **Significant organizational changes** (e.g., mergers, acquisitions, or major restructurings).
- **Implementation of new technologies** that could affect security risk.
- **New legal or regulatory requirements** (e.g., updates to GDPR, NIS2 Directive).
- **After a major security incident** to incorporate lessons learned and improve defenses.

Regulatory Monitoring:

- Changes in **European, national, or international cybersecurity laws** are monitored regularly by the **Compliance and Legal Departments** to trigger policy updates.

10.2 Review and Update Responsibilities

Policy Owner:

- The **Chief Information Security Officer (CISO)** or an assigned **Security Governance Officer** is responsible for coordinating and overseeing the policy review process.

Stakeholder Involvement:

- Reviews involve collaboration among:
    - **IT Security Teams** (technical controls and defenses).
    - **Compliance and Legal Departments** (regulatory requirements).
    - **Human Resources** (employee conduct and awareness training).
    - **Executive Leadership** (strategic security planning and resource allocation).

Employee Communication:

- Any **substantial changes** to the Information Security Policy will be **communicated to all employees**, contractors, and affected third parties.
- Employees must **acknowledge receipt** and **review of updated policies** through formal re-acceptance processes.

10.3 Version Control and Documentation

Version Control Mechanism:

- Each iteration of the policy is assigned a **version number, date of update, and a summary of changes**.
- An archive of previous versions is maintained for **audit and reference purposes**.

Audit Trails:

- Policy reviews and updates are **logged and documented** as part of the organization's **audit readiness requirements** under frameworks such as **ISO/IEC 27001**.

Compliance Validation:

- Updated policies are cross-validated against:
    - ISO/IEC 27001 Information Security Standards.
    - GDPR requirements.
    - NIST Cybersecurity Framework (if applicable).

10.4 Continual Improvement Philosophy

At **Live Now Technology SLU**, we treat information security as a **dynamic and continuous process**, not a one-time compliance task.

We continuously seek to:

- **Adapt** to emerging threats and vulnerabilities.

- **Enhance** the security skills and awareness of employees.
- **Strengthen** technological defenses through innovation and best practices.
- **Promote** a proactive security culture across the organization.

❖ **Commitment Statement:**

"Live Now Technology SLU is dedicated to continual improvement in information security practices, ensuring the ongoing protection of our data, systems, clients, and reputation."

Occupational Health and Safety Policy

1. Introduction & Purpose

At **Live Now Technology SLU**, the health, safety, and well-being of our employees, contractors, visitors, and stakeholders are fundamental to our success.
We recognize that maintaining a safe, healthy, and supportive work environment is not only a **legal and ethical obligation** but also a critical enabler of **productivity, innovation, and employee satisfaction**.

This Occupational Health and Safety (OHS) Policy establishes the company's commitment to:
Preventing work-related injuries, illnesses, and accidents.
Promoting a culture of safety, responsibility, and continuous improvement.
Complying fully with applicable occupational health and safety regulations at the **European** (e.g., **EU Directive 89/391/EEC**) and **Spanish national levels** (e.g., **Ley 31/1995 de Prevención de Riesgos Laborales - PRL**).
Integrating health and safety considerations into all operational and management decisions.

Through this policy, we aim to ensure that all individuals working for or with **Live Now Technology SLU** can perform their duties in a **safe, healthy, and supportive environment**, regardless of whether they are based on-site, remotely, or at a client location.

2. Scope & Applicability

This Occupational Health and Safety Policy applies to:

- **All employees** (permanent, temporary, full-time, part-time, and remote workers).
- **Contractors, freelancers, consultants, and interns** engaged in any company-related activities.
- **Visitors and clients** who access company premises or project sites.

Covered Locations:

- All **Live Now Technology SLU** offices, facilities, and operational locations.
- **Remote work environments**, including employees' home offices when working from home.
- **Client sites** where company employees perform duties under contractual agreements.

Covered Activities:

- Day-to-day work activities (including office work, remote work, fieldwork, and technical services).
- Business travel, conferences, off-site meetings, and training sessions.
- Use of company-provided equipment, vehicles, or digital infrastructure (IT-related work).

All individuals under the scope of this policy are **required to comply with its principles** and **actively contribute to maintaining a safe and healthy work environment**.

3. Company’s Commitment to Health and Safety

Live Now Technology SLU is fully committed to:

Legal Compliance:

- Complying with all applicable health and safety legislation, regulations, and standards, including national Spanish laws and European Union directives.
- Meeting or exceeding industry best practices in occupational health and safety management.

Risk Prevention and Hazard Control:

- Identifying and evaluating workplace hazards proactively.
- Implementing effective preventive and protective measures.
- Investigating all incidents and near-misses to prevent recurrence.

Health Promotion and Well-Being:

- Supporting initiatives that promote **physical, mental, and emotional health**.
- Encouraging **ergonomic best practices**, especially for remote and office-based workers.
- Offering access to **wellness programs and resources** aimed at enhancing work-life balance and preventing occupational stress.

Employee Involvement and Consultation:

- Encouraging open communication and active participation from employees in matters relating to health and safety.
- Establishing formal mechanisms for employees to **report hazards, concerns, and suggestions** confidentially.
- Engaging employees in **health and safety committees or working groups**, when applicable.

Continuous Improvement:

- Setting clear, measurable objectives and targets for health and safety performance.
- Monitoring performance through audits, inspections, and reporting.
- Reviewing this policy periodically and updating it to reflect changes in legislation, organizational activities, and risk landscapes.

Accountability at All Levels:

- Management leads by example and is held accountable for implementing the health and safety policy.
- Every individual shares responsibility for ensuring their own safety and that of their colleagues.

By fostering a strong safety culture, we protect our people, strengthen our organization, and demonstrate our responsibility to society.
“Safety is not just a policy — it is a core value that defines how we work.” 🚀

4. Health and Safety Responsibilities

Occupational health and safety is a **shared responsibility** at **Live Now Technology SLU**. Every individual within the organization has a vital role to play in maintaining a **safe and healthy work environment**.

4.1 Responsibilities of Company Leadership

- Demonstrate **visible and proactive leadership** in promoting health and safety.
- Ensure that **adequate resources (time, personnel, and budget)** are allocated to implement health and safety programs.
- Incorporate health and safety objectives into **business planning and decision-making processes**.
- Foster an environment where **employees feel empowered** to report unsafe conditions or behaviors without fear of retaliation.
- Appoint qualified personnel to manage occupational health and safety responsibilities.

4.2 Responsibilities of Managers and Supervisors

- Ensure that employees under their supervision are **properly trained and equipped** to perform their tasks safely.
- Conduct **regular safety inspections** and **risk assessments** in their areas of responsibility.
- Immediately **address unsafe behaviors or conditions** and initiate corrective actions.
- Support incident investigations by **gathering accurate information** and **participating in root cause analyses**.
- Lead by example by **adhering to all health and safety procedures**.

4.3 Responsibilities of Employees and Contractors

- **Comply with all safety instructions, procedures, and training.**
- **Take reasonable care** of their own health and safety and that of others who may be affected by their actions.
- **Promptly report** any hazards, unsafe practices, or incidents to supervisors or the Health and Safety Officer.
- **Use protective equipment (PPE)** appropriately when required.
- **Participate in health and safety training sessions** and refreshers as required.
- **Cooperate with incident investigations** and safety initiatives.

4.4 Responsibilities of the Health and Safety Officer (or External OHS Service Provider)

- **Develop, implement, and update** the company’s health and safety management system.

- **Advise management** on health and safety compliance, risk mitigation, and best practices.
- **Conduct regular audits, workplace inspections, and risk assessments**.
- **Deliver health and safety training** to all staff.
- **Maintain records of incidents, audits, and inspections**, and track corrective actions.
- **Ensure emergency preparedness**, including evacuation procedures and first aid training.

5. Risk Assessment & Hazard Management

A **proactive approach** to identifying and controlling risks is essential to maintaining a safe work environment.

5.1 Risk Identification and Assessment

- **Periodic risk assessments** are conducted for all company operations, including offices, remote workstations, and project sites.
- **Hazards are identified and documented**, considering physical, ergonomic, psychosocial, and technological risks.
- **Risk levels** (likelihood and severity) are assessed, and mitigation strategies are prioritized accordingly.

5.2 Risk Control and Mitigation

- Apply the **hierarchy of controls** approach:
    1. **Eliminate** the hazard if possible.
    2. **Substitute** with safer alternatives.

3. **Implement engineering controls** (e.g., ergonomic furniture, ventilation systems).
4. **Implement administrative controls** (e.g., safe work procedures, signage).
5. **Use Personal Protective Equipment (PPE)** as a last resort.

5.3 Reporting and Managing Incidents

- All **accidents, near-misses, unsafe conditions, and illnesses** must be **immediately reported**.
- **Incident investigations** are conducted to determine root causes and prevent recurrence.
- Corrective actions are assigned, tracked, and evaluated for effectiveness.

5.4 Documentation and Recordkeeping

- Risk assessments, incident reports, and corrective action plans are **documented and securely stored**.
- Regular reviews of past incidents help identify **patterns and trends** for further risk reduction.

6. Emergency Preparedness and Response

Preparation for emergencies is critical to **minimize harm and disruption** during unexpected events.

6.1 Emergency Procedures

- **Comprehensive emergency plans** (fire evacuation, medical emergencies, natural disasters) are maintained for all sites.

- **Evacuation maps, fire extinguishers, and first aid kits** are clearly marked and readily accessible.
- **Remote workers** are also provided with emergency guidance for their home offices.

6.2 Emergency Response Teams

- Trained **Emergency Response Teams (ERTs)** are designated at each physical site.
- ERTs are responsible for:
    - Coordinating evacuation efforts.
    - Providing basic first aid until professional help arrives.
    - Communicating with emergency services and internal leadership.

6.3 Training and Drills

- **Annual emergency evacuation drills** are conducted at all facilities.
- **First aid training** is mandatory for selected employees at each location.
- Emergency plans are **reviewed and updated annually** or after significant changes (e.g., relocation, expansion).

6.4 Crisis Communication

- In the event of an emergency, clear and **timely communication channels** are established (emails, SMS alerts, internal notification systems).
- Crisis communication roles and escalation paths are **predefined and rehearsed**.

6.5 Post-Emergency Recovery

- After any emergency, a **post-incident review** is conducted to analyze effectiveness and recommend improvements.

- Business Continuity Plans (BCPs) are activated if necessary to ensure operational resilience.

7. Promoting Health, Wellness & Ergonomics

At **Live Now Technology SLU**, we believe that occupational health extends beyond preventing physical accidents — it also encompasses **mental health, ergonomics, and holistic well-being**. We are committed to creating a **supportive, healthy work environment** where employees can thrive physically and mentally.

7.1 Ergonomic Best Practices

- All workstations (office and remote) are designed following **ergonomic standards** to prevent musculoskeletal injuries.
- Ergonomic assessments are offered to employees upon onboarding or upon request.
- Adjustable chairs, monitor stands, keyboards, and other equipment are made available where necessary.
- Guidance for **remote workers** on setting up safe, comfortable home offices is provided through dedicated resources and consultations.

7.2 Mental Health and Well-being

- The company promotes awareness of **mental health issues** and provides resources for stress management, resilience, and work-life balance.
- Employees have confidential access to **mental health support services** (e.g., employee assistance programs, external counselors, or partnerships).
- Workloads and deadlines are managed to avoid **excessive work-related stress**.

7.3 Healthy Work Environment Initiatives

- Encouragement of **regular breaks**, including the use of "micro-breaks" to reduce eye strain and repetitive motion injuries.
- Provision of **healthy lifestyle resources**, including nutrition, exercise, and wellness programs.
- Support for **flexible working arrangements** where possible to accommodate personal needs and promote work-life integration.

8. Training and Awareness

Training is essential to **empower employees** to recognize hazards, understand safe practices, and respond effectively in emergencies.

8.1 Health and Safety Training Requirements

- **Mandatory onboarding training** on health, safety, and emergency procedures for all new hires.
- **Annual refresher training** for all employees to reinforce critical safety concepts and update them on any policy or procedure changes.
- **Role-specific training** for employees performing higher-risk activities (e.g., server room maintenance, site visits, fieldwork).

8.2 Awareness and Communication Campaigns

- Ongoing **awareness initiatives** (e.g., posters, newsletters, webinars) promote safe behaviors and highlight emerging risks.
- **World Health and Safety Days**, mental health awareness weeks, and other events are celebrated internally.

8.3 Emergency Drill Training

- Regular **fire drills**, evacuation practices, and first aid response drills are conducted to ensure preparedness.
- Remote workers receive guidelines on how to respond to emergencies in their own working environments.

8.4 Continuous Improvement Through Training Feedback

- Feedback from employees after training sessions is collected and used to **improve training content and delivery**.

9. Compliance and Continuous Improvement

Compliance is not static — **continuous improvement** is vital to ensure the highest standards of occupational health and safety.

9.1 Regulatory Compliance

- **Live Now Technology SLU** complies with:
  - **EU Directive 89/391/EEC** on the introduction of measures to encourage improvements in the safety and health of workers.
  - **Ley 31/1995 de Prevención de Riesgos Laborales** (Spanish Occupational Risk Prevention Act).
  - Relevant ISO standards (such as **ISO 45001 Occupational Health and Safety Management Systems**, where applicable).

9.2 Regular Health and Safety Audits

- Periodic audits are conducted to identify gaps, risks, and opportunities for improvement.
- Corrective actions are prioritized and implemented promptly following audit findings.

9.3 Incident and Hazard Reporting Mechanism

- All employees are encouraged to **report hazards, incidents, and near misses confidentially**.
- All reports are logged, investigated, and used to improve safety measures.

9.4 Management Reviews and Improvement Plans

- Health and Safety performance is **reviewed annually by senior leadership**.
- Performance metrics (e.g., incident rates, audit findings, training completion rates) guide continuous improvement initiatives.

10. Acknowledgment and Enforcement

Ensuring a safe workplace requires the **active participation and commitment** of all individuals associated with the company.

10.1 Employee Acknowledgment

- All employees and contractors must **acknowledge receipt** of the Occupational Health and Safety Policy during onboarding.
- By acknowledging the policy, individuals agree to:
    - **Comply** with all safety procedures.
    - **Take proactive steps** to protect themselves and their colleagues.

  - **Report any health and safety risks or violations** immediately.

10.2 Enforcement and Disciplinary Actions

- Failure to comply with this policy, or any deliberate disregard of health and safety procedures, may result in **disciplinary action**, up to and including:
  - Verbal or written warnings.
  - Suspension.
  - Termination of employment or contract.
  - Legal action if applicable under labor or criminal laws.

10.3 Commitment to Shared Responsibility

- Health and safety is a **collective effort** — a shared responsibility between management, employees, contractors, and visitors.

- By working together, we create a **safer, healthier, and more productive workplace** for everyone.

Environmental Policy

1. Introduction & Purpose

At **Live Now Technology SLU**, we recognize that environmental responsibility is essential to ensuring a **sustainable future**, and we are committed to **minimizing the environmental impact** of our operations, services, and supply chain.

As a digital engineering and consulting firm operating across Europe, we may not be a heavy polluter in the traditional sense, but we understand the significant **indirect impacts** we generate through **energy consumption, digital infrastructure, travel, and procurement**.

This Environmental Policy outlines our **principles, objectives, and actions** for protecting the environment and contributing to global efforts such as the **European Green Deal**, the **United Nations Sustainable Development Goals (SDGs)**, and compliance with **environmental legislation** at both **EU and national levels**.

Our commitment is not only to comply with environmental laws but to **go beyond compliance** by embedding sustainability into the **core of our culture, decision-making processes, and operations**.

2. Scope & Applicability

This Environmental Policy applies to:
All operations and activities carried out by Live Now Technology SLU, including administrative, technical, consulting, and remote work functions.
All employees, contractors, consultants, and interns, whether working on-site or remotely.
Third-party vendors, suppliers, and service providers, particularly those with environmental impacts connected to our business.

The policy is relevant to all environmental aspects, including but not limited to:

- **Energy consumption** in offices, server infrastructures, and employee workstations.

- **Greenhouse gas emissions** related to energy use, commuting, and travel.
- **Digital sustainability**, including server load, data storage, and computational efficiency.
- **Waste generation**, including e-waste and office materials.
- **Procurement**, including the environmental standards of purchased products and vendor sustainability practices.

This policy is also aligned with **ISO 14001:2015 Environmental Management Systems**, and serves as the foundation for our environmental management efforts and improvement plans.

3. Environmental Commitments & Principles

At the core of our environmental efforts lies a firm set of commitments. These guide our **strategy, decision-making, employee behavior, and vendor relationships**:

3.1 Compliance and Beyond

- Ensure full compliance with **applicable environmental laws, directives, and regulations** in every country where we operate.
- Monitor legislative changes and proactively update our practices accordingly.
- Where feasible, **adopt stricter internal standards** that go beyond legal minimums.

3.2 Pollution Prevention and Impact Reduction

- Prevent pollution by **reducing waste, minimizing resource consumption, and eliminating hazardous substances** from operations.

- Encourage **paperless workflows**, digital documentation, and efficient cloud computing.
- Promote **remote collaboration** to reduce commuting and travel emissions.

3.3 Resource Efficiency and Energy Management

- Strive for **efficient use of energy, water, and materials**, especially in office operations and IT infrastructure.
- Migrate services to **energy-efficient and carbon-neutral cloud providers** wherever possible.
- Implement strategies to reduce the **carbon footprint** associated with digital tools, platforms, and internal infrastructure.

3.4 Circular Economy & Sustainable Procurement

- Encourage reuse, repair, and recycling of **electronic and office equipment**.
- Give preference to **eco-certified products and vendors** with transparent sustainability policies.
- Extend product life cycles and reduce overconsumption of resources.

3.5 Transparency, Collaboration & Continuous Improvement

- Monitor environmental performance regularly and **set measurable environmental objectives**.
- Continuously improve through **audits, reviews, and employee engagement**.
- Communicate transparently with stakeholders and clients regarding our sustainability journey and results.

At Live Now Technology SLU, **sustainability is not an isolated effort —** it is an integral part of our identity and commitment to being a **responsible and future-ready company**.

4. Key Focus Areas

To ensure effective implementation of our environmental commitments, **Live Now Technology SLU** concentrates its sustainability efforts across the following strategic pillars:

4.1 Energy Efficiency and Carbon Emissions

- Optimize energy usage in offices and digital infrastructure.
- Prioritize the use of **renewable energy providers** in rented offices and cloud services.
- Encourage **smart use of lighting, heating, and cooling systems**, supported by automation and energy-saving devices.
- Monitor carbon emissions from company operations and **identify reduction opportunities** annually.
- Use **carbon offset programs** where direct reduction is not feasible.

4.2 Waste Management and Recycling

- Apply **waste reduction principles** to all areas of operation.
- Implement **selective waste separation systems** in company offices (paper, plastics, e-waste, organic).
- Minimize **single-use materials** and promote **reusable office supplies**.
- Ensure that obsolete equipment is disposed of through **certified e-waste recycling programs**.

4.3 Sustainable Procurement

- Give preference to **vendors and suppliers** who follow environmentally sustainable practices.
- Evaluate suppliers based on their **environmental certifications, emissions, and labor practices**.
- Procure **energy-efficient, eco-labeled hardware**, recycled materials, and low-impact consumables.
- Avoid procurement of **non-essential physical goods**, especially if digital alternatives exist.

4.4 Green IT and Digital Sustainability

- Reduce energy consumption and emissions from **data storage and processing** through:
    - Use of **efficient cloud services (e.g., with ISO 50001, ISO 14001 or carbon-neutral guarantees)**.
    - **Optimizing software performance** to reduce computational load.
    - **Cleaning up digital storage** periodically to reduce unnecessary cloud usage.
- Raise awareness of the **environmental cost of digital infrastructure** (data centers, training large models, excessive email storage, etc.).

4.5 Business Travel and Remote Work

- Encourage **remote-first work** to reduce emissions from commuting and travel.
- Establish policies to **limit business travel** to essential purposes only.
- Prioritize **train travel over flights** for regional transportation.

- Use virtual meetings and collaboration tools to replace physical events where possible.

5. Roles & Responsibilities

Environmental responsibility is shared across the organization, with specific roles defined to ensure accountability:

5.1 Company Leadership

- Set the tone and direction of environmental policy through strategic decision-making.
- Allocate **resources and budget** for environmental initiatives.
- Ensure compliance with legal and regulatory frameworks at national and EU levels.
- Approve and monitor key performance indicators (KPIs) related to sustainability.

5.2 Employees

- Apply environmental principles in their day-to-day tasks (e.g., reducing waste, turning off unused devices).
- Use remote work and travel policies responsibly to limit environmental impact.
- Report suggestions, risks, or issues related to environmental practices.
- Participate in training and awareness campaigns.

5.3 Environmental Coordinator (or Assigned Officer)

- Develop and maintain the **environmental management system**.
- Track and report **performance indicators** and compliance metrics.

- Liaise with departments and suppliers to integrate environmental standards.
- Coordinate awareness campaigns, audits, and policy reviews.

5.4 Vendors and Contractors

- Must adhere to **environmental requirements** included in contracts.
- Provide proof of certifications or sustainability commitments upon request.
- Collaborate in reducing packaging, emissions, and waste where applicable.

6. Monitoring, Compliance & Continuous Improvement

To ensure the effectiveness of our environmental management efforts, Live Now Technology SLU establishes a robust framework for **measuring, reviewing, and continuously improving** our environmental impact.

6.1 Performance Monitoring

- Define and track **Environmental Key Performance Indicators (eKPIs)**, such as:
    - Electricity and energy consumption.
    - Carbon emissions from travel and digital services.
    - Waste volumes and recycling ratios.
    - Procurement impact metrics.
- Annual reporting and analysis of results and progress.

6.2 Legal and Regulatory Compliance

- Ensure adherence to applicable environmental laws and directives:
    - **EU Directive 2004/35/EC** on environmental liability.
    - **Spanish Law 26/2007** on environmental responsibility.
    - ISO 14001 standards where applicable.
- Conduct **annual compliance audits** to detect gaps and implement corrective actions.

6.3 Policy Review and Continuous Improvement

- This policy is reviewed at least **once per year** or after significant operational changes.
- The review includes **evaluation of current initiatives, stakeholder feedback, and regulatory updates**.
- Corrective and preventive measures are implemented as needed.

6.4 External Communication and Transparency

- Environmental performance may be included in **annual sustainability disclosures**.
- Clients and stakeholders may request documentation or KPIs related to environmental practices.

7. Awareness, Engagement & Communication

A strong environmental policy requires not only defined commitments, but also **active engagement and participation** across the entire organization. At **Live Now Technology**

SLU, we strive to build a culture where sustainability is **understood, practiced, and promoted by all employees and stakeholders**.

7.1 Environmental Training & Education

- All employees receive **environmental awareness training** as part of the onboarding process.
- Periodic **refresher sessions and e-learning modules** are provided to keep staff informed about new practices, regulations, and internal goals.
- Specific teams (e.g. procurement, operations, infrastructure) may receive **role-specific environmental training** related to their functions.

7.2 Employee Engagement & Participation

- Employees are encouraged to **submit suggestions or initiatives** that support sustainability goals.
- Company-wide campaigns, such as **Green Weeks** or **Digital Cleanup Days**, are organized to reinforce behavioral change.
- Internal communications (newsletters, Slack channels, intranet) include regular content on sustainability tips, achievements, and opportunities.

7.3 External Communication & Stakeholder Collaboration

- We are transparent with clients, suppliers, and partners about our environmental objectives and progress.
- Sustainability commitments may be **included in proposals, supplier contracts, and client documentation**, where appropriate.
- We support **collaborative efforts** with external partners (industry groups, NGOs, regulatory bodies) to amplify our environmental impact.

7.4 Promoting a Culture of Sustainability

- Sustainability is not treated as an isolated initiative, but as an **integral part of how we work, think, and grow**.
- Managers are expected to **lead by example**, incorporating environmental criteria into planning, procurement, and team activities.
- Remote workers and hybrid teams are equally involved through virtual campaigns and guidance on home-based sustainability practices.

8. Acknowledgment and Policy Governance

To ensure effective implementation of this policy, **Live Now Technology SLU** defines clear governance, responsibility, and enforcement mechanisms.

8.1 Acknowledgment of Responsibility

- All employees and contractors must **acknowledge their understanding of this Environmental Policy** and commit to complying with its principles.
- The policy is included in **employee onboarding documentation**, and periodic reaffirmation may be required during annual reviews or audits.

8.2 Policy Availability and Accessibility

- This policy is made available to all employees, clients, suppliers, and stakeholders through our internal documentation systems and company website (where applicable).
- Printed or digital copies may be provided upon request for compliance or project-related documentation.

8.3 Enforcement and Non-Compliance

- Violations of this policy may result in **corrective or disciplinary action**, depending on the nature and severity of the breach.

- Managers and the Environmental Coordinator are responsible for investigating non-compliance, issuing recommendations, and ensuring resolution.

8.4 Policy Review and Update Cycle

- This policy is reviewed **annually** and updated as needed to reflect:
    - Changes in legislation or best practices.
    - Operational changes within the company.
    - Environmental performance results or audit findings.

“Environmental responsibility is a shared obligation. Through awareness, innovation, and accountability, we can make a lasting difference for our planet and future generations.” 🌍

Quality Policy

1. Introduction & Purpose

At **Live Now Technology SLU**, quality is not just a goal — it is a core value that defines our identity, our work ethic, and our long-term vision. We are dedicated to delivering **high-reliability services and solutions** that meet or exceed the expectations of our clients, partners, and stakeholders.

This Quality Policy sets out our strategic commitment to:

- **Providing services that are technically sound, compliant, and aligned with client mission goals**.
- Fostering a company culture based on **continuous improvement, operational excellence, and attention to detail**.
- Aligning our quality management practices with **international standards**, such as **ISO 9001:2015**.

In a business environment driven by **data processing, software development, system engineering, and compliance with European space and environmental programs**, the **reliability and traceability** of our deliverables is essential. Our clients depend on us for solutions that are **secure, scalable, well-documented, and rigorously validated** — and we are committed to earning and maintaining that trust.

2. Scope & Applicability

This Quality Policy applies to:
All activities, processes, and services carried out by Live Now Technology SLU.
All employees, contractors, and business units, regardless of location, whether working on internal operations, client projects, or collaborative initiatives.
All project phases, from pre-sales engineering and system design to delivery, maintenance, and post-deployment support.

The policy covers:

- **Software engineering and development** (including prototypes, operational systems, and scientific software).

- **Data processing and analytics solutions**, particularly in Earth observation and environmental monitoring contexts.

- **Systems engineering**, including design, verification, integration, and validation phases.

- **Project and service management**, including client communications and documentation.

- **Third-party/vendor interactions**, where quality dependencies exist.

Every person involved in the delivery of our services — whether internally or externally — is expected to adhere to the **quality standards, procedures, and ethical practices** defined under this policy.

3. Quality Commitments

Live Now Technology SLU is committed to maintaining a **robust quality culture** based on the following principles:

3.1 Customer Satisfaction

- We place **client needs at the center** of our work.

- We strive to deliver **on time, within scope, and at the expected level of performance**.

- We actively seek feedback and use it to improve services and relationships.

- We aim to become a **trusted long-term partner**, not just a one-time provider.

3.2 Compliance with Standards & Requirements

- We adhere to **contractual, legal, and regulatory requirements**, including applicable European and international standards (e.g., ECSS, ISO 9001, GDPR).

- We maintain **traceability, reproducibility, and validation** across all technical deliverables.

- We implement **quality controls and formal reviews** at each critical project milestone.

3.3 Continuous Improvement

- We regularly **review our internal processes and tools** to identify and eliminate inefficiencies.

- We promote a mindset of **learning, sharing knowledge, and evolving practices** across teams.

- Non-conformities are addressed through **structured root-cause analysis and corrective action plans**.

- Innovation and excellence are encouraged and supported in all areas of the company.

3.4 Reliability, Integrity & Professionalism

- We ensure that our outputs are **technically accurate, secure, and reliable**.

- We communicate transparently with our clients and maintain **professional integrity** in every aspect of delivery.

- Quality is not just checked — it is **engineered into every stage** of our work.

4. Quality Management System (QMS)

At **Live Now Technology SLU**, our Quality Management System (QMS) is designed to ensure that all projects, processes, and deliverables consistently meet both **internal**

performance standards and **external contractual and regulatory requirements**.

4.1 Key Components of the QMS

- **Documented processes** for software development, data engineering, system design, project management, and validation.
- **Risk-based thinking** and preventive approaches applied across the lifecycle of each service or product.
- Use of **configuration management and version control systems** to ensure traceability.
- Integration of **quality checkpoints**, reviews, and audits into project plans and delivery milestones.

4.2 Digital Tools & Automation

- Use of **project tracking platforms (e.g., Jira, Git, internal dashboards)** to manage tasks and quality gates.
- **Automated testing, CI/CD pipelines**, and code review workflows are employed to reduce errors and improve repeatability.
- Documentation and deliverables are versioned and stored securely, with **access control and audit trails**.

4.3 Alignment with ISO 9001 and Industry Best Practices

- The QMS aligns with the **ISO 9001:2015** standard for Quality Management Systems.
- Where applicable, quality controls are tailored to comply with **ECSS standards** (for space systems) and other domain-specific frameworks.
- The QMS evolves through **feedback loops, lessons learned sessions, and internal audits**.

5. Roles & Responsibilities

5.1 Executive Management

- Define the company's **quality objectives and vision**.
- Provide **resources, leadership, and visibility** for the QMS.
- Review performance data and **validate strategic improvements** annually.

5.2 Project Managers & Team Leads

- Ensure **project execution adheres to defined quality procedures**.
- Monitor deliverables for **technical completeness, client satisfaction, and contractual compliance**.
- Facilitate **quality reviews and sign-offs** at key stages.
- Report issues or deviations proactively and drive resolution.

5.3 Quality Assurance Function / Designated Officer

- Maintain and update the **Quality Management System documentation**.
- Conduct **periodic internal audits and quality reviews**.
- Track and analyze non-conformities and improvement opportunities.
- Support certification efforts and ensure alignment with external standards.

5.4 All Employees & Contractors

- Understand and follow the QMS procedures relevant to their roles.
- Take personal responsibility for **the quality of their work**.
- Flag any quality-related risks, bottlenecks, or deviations to their team leads.

- Participate actively in **lessons learned, retrospectives, and continuous improvement efforts**.

6. Monitoring, Evaluation & Continuous Improvement

Our quality strategy is driven by **data, measurement, and accountability**.

6.1 Key Quality Indicators (KQIs)

- Timely delivery of project milestones.
- Defect density and issue resolution time.
- Customer satisfaction metrics (feedback, surveys, NPS).
- Internal process conformance and audit scores.
- Effectiveness of corrective and preventive actions (CAPA).

6.2 Internal Audits & Reviews

- **Planned audits** are conducted regularly to assess compliance and detect inefficiencies.
- **Post-project reviews and retrospectives** help capture insights and improvements.
- Deviations and non-conformities are **documented, tracked, and resolved** through a structured process.

6.3 Continuous Learning & Process Optimization

- Best practices and reusable assets (e.g., templates, checklists, tools) are shared across teams.

- Root cause analysis (RCA) is applied systematically to prevent reoccurrence of critical issues.

- Staff are encouraged to **propose process improvements and innovative approaches**.

7. Policy Review & Acknowledgment

7.1 Policy Review Cycle

- This Quality Policy is reviewed **annually** by senior management and the designated quality officer.

- It may be updated earlier in response to:

    - Changes in strategy or operational scope.

    - Audit findings or significant process changes.

    - Regulatory updates or client requirements.

7.2 Acknowledgment and Compliance

- All employees and collaborators must **read, understand, and commit to this Quality Policy** as part of onboarding.

- Ongoing acknowledgment may be requested during annual reviews, compliance assessments, or certification audits.

7.3 Policy Availability

- The policy is available via internal documentation systems and may be shared with clients, partners, and certification bodies upon request.

- It reflects the **company's commitment to transparency, reliability, and professional excellence**.

“At Live Now Technology SLU, quality is not a single task — it is the way we operate, deliver, and grow. It empowers us to meet the high standards of our clients and the integrity of our mission.” ✅

Business Continuity Policy and/or Information Security Crisis Management Plan

1. Introduction & Purpose

At **Live Now Technology SLU**, we recognize that uninterrupted service delivery, data integrity, and operational resilience are vital to our business success and to the trust our clients place in us. As a provider of engineering, software, and data processing solutions for high-reliability environments — including European space and environmental programs — we must ensure that our services can **withstand disruption and recover quickly from crises**.

This policy establishes our framework for:

- Ensuring **business continuity** in the face of internal and external disruptions.
- Responding swiftly and effectively to **information security incidents** and **cyber threats**.
- Protecting our **clients, infrastructure, intellectual property, and reputation**.

This policy aligns with industry best practices and standards, including:

- **ISO 22301** – Business Continuity Management Systems (BCMS)
- **ISO/IEC 27035** – Information Security Incident Management
- **NIST SP 800-61** – Computer Security Incident Handling Guide

The purpose of this policy is to **prevent, prepare for, respond to, and recover from disruptive events**, whether caused by cyberattacks, system failures, natural disasters, or human error — and to **maintain trust, compliance, and operational integrity** at all times.

2. Scope & Applicability

This policy applies to:

- **All Live Now Technology SLU operations, employees, contractors, and IT systems**, whether on-site, remote, or cloud-based.
- **Critical business functions**, including software delivery, data processing, technical consultancy, system support, and project management.
- All stages of **incident management and continuity planning**, from threat detection to service restoration.

The policy is applicable to both:

- **Business Continuity Management (BCM)**: Ensuring the organization can maintain essential services during and after a disruption.

- **Information Security Crisis Management (ISCM)**: Detecting, responding to, and recovering from security breaches and cyber incidents.

This policy is **integrated with** the following internal frameworks:

- Information Security Policy

- Risk Management Policy

- Quality Policy

- Data Protection (GDPR) Framework

- Internal Communication Protocols

3. Objectives of Business Continuity

The primary objectives of this Business Continuity and Crisis Management Policy are to:

3.1 Protect People and Assets

- Safeguard the health and safety of employees and stakeholders during operational disruptions.
- Protect data, systems, infrastructure, and physical assets from damage or loss.

3.2 Minimize Business Impact

- Ensure that **critical operations can continue** with minimal interruption.
- Reduce downtime and data loss through pre-defined **Recovery Time Objectives (RTOs)** and **Recovery Point Objectives (RPOs)**.
- Limit the financial, legal, and reputational impact of crises.

3.3 Rapid Response and Recovery

- Provide clear procedures and escalation paths to **respond swiftly and effectively** to incidents.
- **Restore normal operations within predefined timeframes**, supported by redundancy, backups, and external support when needed.

3.4 Maintain Trust and Compliance

- Meet obligations to clients, partners, and regulators — including **contractual service level agreements (SLAs)**.
- Comply with data protection regulations (e.g., GDPR) and incident reporting requirements (e.g., notification within 72 hours of a breach).

3.5 Continuous Readiness

- Regularly test and review business continuity and incident response plans.
- Foster a **resilience culture** across the organization, ensuring that staff are aware, trained, and prepared.

4. Business Continuity Planning (BCP)

Our **Business Continuity Plan (BCP)** is designed to ensure the continuity of critical operations, even in the face of disruptive events. The plan outlines strategies for **preparedness, mitigation, response, and recovery** across key functions.

4.1 Identification of Critical Business Functions

Each department is responsible for identifying its **mission-critical activities** and the **resources** necessary to maintain or restore them. These typically include:

- Access to source code and repositories.
- Client-facing digital services and hosting.
- Data processing pipelines and cloud infrastructure.
- Communication and collaboration tools.
- Legal and compliance operations.

4.2 Recovery Objectives

- **Recovery Time Objective (RTO):** The maximum acceptable time to restore a service after disruption.
- **Recovery Point Objective (RPO):** The maximum tolerable data loss expressed in time.

These are defined per system or process and documented within the BCP.

4.3 Continuity Strategies

- Use of **cloud-based infrastructure with high availability (HA)** and regional redundancy.
- **Remote working capabilities** for all essential staff.
- Secure and frequent **data backups**, stored in off-site or cloud environments.

- Pre-approved **alternative suppliers** for critical services or infrastructure.
- **Pre-configured virtual environments** for development and operations.

4.4 BCP Ownership and Maintenance

- Each department nominates a **Business Continuity Coordinator**.
- The **BCP is reviewed at least annually**, and after major incidents or organizational changes.
- All employees are trained on their responsibilities under the BCP.

5. Information Security Incident & Crisis Management

The **Incident Response Plan (IRP)** defines how to detect, respond to, and recover from **cybersecurity incidents** or **data breaches**. It ensures that all incidents are handled efficiently and in compliance with legal and contractual obligations.

5.1 Incident Detection and Reporting

- All employees are required to report any suspected incident **immediately** to the designated security team.
- Incident categories include:
  - Unauthorized access or data leakage
  - Ransomware or malware infection
  - Phishing or social engineering attempts
  - Compromise of credentials or authentication systems

5.2 Incident Response Team (IRT)

- The IRT includes IT Security, Legal, Communications, and Executive Management.
- Responsibilities include:
  - **Assessing and containing** the incident
  - Preserving evidence
  - **Coordinating remediation and recovery**
  - Communicating with affected stakeholders

5.3 Escalation and Classification

Incidents are classified by **severity level**, with clear escalation paths:

- **Low:** No impact on operations.
- **Medium:** Temporary disruption or limited data exposure.
- **High:** Major outage, sensitive data breach, regulatory exposure.

Each level has predefined **response timelines** and required actions.

5.4 Legal and Regulatory Obligations

- All personal data breaches are reported to relevant authorities in compliance with **GDPR Article 33**.
- Clients affected by the incident are notified according to contractual SLAs.

6. Communication During Disruption

Effective communication is essential for maintaining **trust and control** during a disruptive event.

6.1 Internal Communication

- Emergency contact trees and secure channels (e.g., Signal, encrypted email) are maintained.
- Crisis-specific internal bulletins inform staff of actions and updates.
- Departmental leads coordinate communication with their teams.

6.2 External Communication

- A **Designated Spokesperson** handles all client and media communications.
- Clients are informed proactively if their services or data may be impacted.
- Communication templates are maintained for:
  - Service interruption notices
  - Data breach notifications
  - Reassurance and mitigation status updates

6.3 Communication Platforms

- Company website or status page (if available)
- Email newsletters to clients or stakeholders
- Secure portals for documentation (e.g., incident reports)

7. Testing, Maintenance & Review

To ensure effectiveness, the Business Continuity and Incident Response Plans must be **tested, maintained, and continuously improved**.

7.1 Regular Testing

- **Annual full-scale continuity simulations** (e.g., data center failure, ransomware scenario).
- Periodic **tabletop exercises** to simulate response procedures.
- **Post-exercise reviews** with action items and documented lessons learned.

7.2 Maintenance and Plan Updates

- Plans are reviewed at least **annually**, or when:
    - Critical systems change
    - Organizational structure changes
    - Legal or regulatory frameworks are updated
    - After any major disruption or incident

7.3 Employee Awareness and Training

- All staff are trained on incident recognition, reporting, and recovery protocols.
- Targeted training for:
    - Security response teams
    - Project managers
    - Client support personnel

“Resilience is not built during a crisis — it is built through preparation. At Live Now Technology SLU, we commit to staying operational, responsive, and trustworthy even in the face of disruption.”

Security Incident Response Procedure

1. Introduction & Purpose

At **Live Now Technology SLU**, ensuring the **confidentiality, integrity, and availability** of data and systems is a fundamental priority. As a company operating in high-reliability environments such as **scientific software, system engineering, and Earth observation data processing**, our ability to detect and respond to security incidents is crucial to maintaining client trust, regulatory compliance, and operational resilience.

The **Security Incident Response Procedure (SIRP)** provides a **structured and standardized approach** for detecting, managing, mitigating, and learning from information security incidents. This procedure supports our broader **Information Security Policy**, **Business Continuity Plan**, and our compliance obligations under **ISO/IEC 27001**, **ISO/IEC 27035**, and the **General Data Protection Regulation (GDPR)**.

This document is intended to:

- Minimize the impact of security breaches and system compromises.
- Ensure a consistent, repeatable process for all types of security incidents.
- Enable fast decision-making, legal compliance, and client communication.
- Integrate lessons learned into our **continuous improvement framework**.

2. Scope & Definitions

2.1 Scope

This procedure applies to:

- **All information systems, infrastructure, and services** managed or used by Live Now Technology SLU.

- **All employees, contractors, external collaborators**, and **third-party service providers**.
- All incidents involving potential or actual breaches of:
  - **Data confidentiality**
  - **System integrity**
  - **Service availability**
  - **Legal or regulatory obligations**

It includes incidents affecting:

- Internal corporate systems (email, HR, finance)
- Project environments (client-specific data or software)
- Cloud platforms, APIs, and source code repositories (e.g. GitHub, AWS, Firebase)

2.2 Definitions

- **Security Incident:** Any event or series of events that compromises or threatens to compromise the confidentiality, integrity, or availability of systems or data.
- **Breach:** A confirmed event where data or systems have been accessed, disclosed, altered, or destroyed without authorization.
- **Incident Response (IR):** The coordinated activities to identify, contain, mitigate, investigate, and recover from a security incident.
- **CSIRT (Computer Security Incident Response Team):** A designated group responsible for managing the incident lifecycle.
- **RCA (Root Cause Analysis):** A structured process to determine the underlying cause(s) of an incident.

3. Objectives of the Incident Response Procedure

The main objectives of the Security Incident Response Procedure are to:

3.1 Enable Rapid Detection and Containment

- Ensure that all employees and systems can **quickly detect anomalies or threats**.
- Apply **real-time monitoring, alerting, and logging mechanisms** to critical systems and services.
- Contain the impact to prevent escalation or lateral movement of attacks.

3.2 Standardize Response Procedures

- Provide a **clear step-by-step process** for responding to incidents across all teams and locations.
- Ensure consistent classification, escalation, and documentation of each case.
- Define **roles, responsibilities, and escalation paths** from the moment an incident is reported.

3.3 Maintain Regulatory and Contractual Compliance

- Guarantee compliance with **GDPR Article 33**, including:
    - Reporting personal data breaches to authorities within **72 hours**.
    - Notifying affected clients or users when required.
- Ensure contractual SLAs with clients are respected during incident response.

3.4 Protect Stakeholder Trust and Company Reputation

- Maintain transparency and professionalism in communication during incidents.

- Reassure clients and partners that **effective controls, investigation, and recovery** are in place.

3.5 Support Continuous Improvement

- Perform **post-incident reviews** to identify root causes, process failures, and future prevention strategies.

- Update policies, procedures, and training based on real incidents and threat intelligence.

4. Incident Classification & Prioritization

Classifying incidents accurately is key to determining the appropriate **response strategy, resource allocation, and communication requirements**.

4.1 Classification Criteria

Incidents are classified based on four dimensions:

1. **Impact on Confidentiality, Integrity, or Availability (CIA)**

2. **Scope of affected systems or users**

3. **Legal/regulatory implications** (e.g. personal data involved)

4. **Potential reputational or financial damage**

4.2 Severity Levels

Severity	Description	Examples

Critical	Severe disruption of core services, confirmed data breach, major regulatory risk	Ransomware affecting cloud infrastructure, breach of client data
High	Partial service outage, credential compromise, unauthorized access	Suspicious remote login to admin console
Medium	Isolated system compromise, phishing click with no execution	Infected user laptop with no access to internal systems
Low	Attempted but failed attack, misconfiguration with no data exposure	Port scan, unsuccessful brute force attack

4.3 Priority Response Windows

Each severity level has a corresponding **Response Time Objective (RTO)**:

- **Critical:** < 1 hour
- **High:** < 4 hours
- **Medium:** < 24 hours
- **Low:** < 72 hours

5. Incident Handling Process (Detection to Closure)

5.1 Phase 1: Detection & Reporting

- Security events are **monitored via automated systems, logs, alerts**, and user reporting.
- All employees must report suspicious activity immediately to the **CSIRT** via secure channels.
- An initial triage is performed to determine validity and potential severity.

5.2 Phase 2: Containment

- For confirmed incidents, the goal is to **limit spread and damage**:
  - Isolate affected endpoints or services.
  - Revoke or reset compromised credentials.
  - Disable vulnerable accounts or firewall rules if needed.

5.3 Phase 3: Eradication & Mitigation

- Remove malicious components (e.g., malware, backdoors).
- Patch exploited vulnerabilities or fix misconfigurations.
- Review and cleanse logs, cloud objects, or network artifacts.

5.4 Phase 4: Recovery

- Restore affected services and systems using **clean backups**.
- Conduct **system validation** and reintegration with production.
- Monitor closely post-recovery to detect reinfection or related attacks.

5.5 Phase 5: Documentation & Closure

- Complete full incident report: timeline, impact, actions, affected parties.
- Log incident in internal system with tags and severity.
- Trigger **root cause analysis (RCA)** for critical and high severity incidents.

6. Incident Response Roles & Responsibilities

A well-defined team structure ensures **swift and coordinated response**.

6.1 Computer Security Incident Response Team (CSIRT)

Led by the **Information Security Officer**, includes:

- **IT Operations**
- **Cloud Infrastructure / DevOps**
- **Legal / Compliance**
- **Communications Lead**
- **Executive Sponsor (optional for critical cases)**

6.2 Role Responsibilities

Role	Responsibilities
Incident Manager	ordinates all response efforts, assigns tasks, manages status tracking
Technical Lead	alyzes root cause, applies patches/fixes, and restores systems
Compliance Officer	Ensures regulatory reporting (e.g., GDPR), documents decisions
mmunications Lead	Manages stakeholder updates, external messaging, client alerts
Executive Sponsor	proves crisis-level decisions, liaises with legal counsel if needed

6.3 Availability & On-Call

- A **rotating on-call roster** is maintained for incident response team availability.
- **Escalation paths and contact trees** are defined and tested quarterly.

7. Communication & Escalation Protocols

Clear and timely communication is essential during a security incident to reduce confusion, maintain stakeholder confidence, and comply with legal obligations.

7.1 Internal Communication

- All employees are required to report suspicious activities or confirmed incidents **immediately** via secure internal channels (e.g., dedicated email alias, encrypted chat).
- The **CSIRT coordinates updates** internally during ongoing incidents, using predefined notification templates.
- Weekly updates are issued for long-running investigations or recovery phases.

7.2 Escalation Procedures

- Incidents are escalated according to **severity level and impact scope**:
    - **Medium or higher** must be reported to the **Executive Sponsor** and Compliance Officer.
    - **Critical incidents** trigger an **emergency CSIRT meeting**, including senior leadership.
- Escalation trees and response timelines are documented and rehearsed quarterly.

7.3 External Communication

- The **Designated Communications Lead** is the only person authorized to:
    - Notify clients of service disruption or potential data impact.
    - Communicate with regulators (e.g., **AEPD** in Spain, **CNIL** in France).
    - Respond to press/media inquiries.
- Pre-approved **notification templates** are used for:
    - Service interruption notices.
    - Breach disclosure notices.
    - GDPR-mandated notifications (within 72 hours).

7.4 Confidentiality and Integrity of Messaging

- All incident-related communications are stored securely.
- Encryption is used for:
    - Sending reports to clients.
    - Internal chat and email if incident content is sensitive.
- All documentation is restricted to “need-to-know” personnel.

8. Post-Incident Activities (Lessons Learned, RCA, Documentation)

After any incident, especially one rated **Medium or higher**, the company conducts a structured **post-incident review (PIR)**.

8.1 Root Cause Analysis (RCA)

- RCA is conducted by the Technical Lead and Incident Manager.

- Focuses on identifying:
  - The initial entry point or vulnerability exploited.
  - Gaps in detection or delayed response.
  - Contributing process failures or miscommunications.
- RCA conclusions are formally documented and reviewed with relevant teams.

8.2 Corrective and Preventive Actions (CAPA)

- All incidents result in a CAPA plan including:
  - Immediate remediation of vulnerabilities.
  - System or process improvements.
  - Updates to documentation or security controls.
  - Internal training updates, if human error was involved.

8.3 Lessons Learned

- Cross-team **debrief sessions** are held within 7 days of incident resolution.
- Key findings are shared (anonymized if necessary) with employees as awareness material.
- Involvement of HR and Legal if the incident has disciplinary or contractual implications.

8.4 Documentation

- Each incident is recorded in the **incident log system** with:
  - Timestamped timeline

  - Involved parties
  - Severity and impact
  - Full technical and procedural summary
- Logs are reviewed quarterly to identify trends and recurring threats.

9. Policy Review & Continuous Improvement

To remain effective and aligned with emerging threats and regulations, the Security Incident Response Procedure is:

9.1 Reviewed and Updated Annually

- The **Information Security Officer** ensures the procedure is updated:
  - After major incidents.
  - In response to audit findings.
  - When there are changes to infrastructure, legal obligations, or services.

9.2 Audited and Tested

- The procedure is subject to:
  - **Annual internal audits**
  - **Penetration tests** to validate detection and response capabilities.
  - Simulated attack drills (e.g., phishing simulation, ransomware tabletop).

9.3 Trained and Enforced

- All employees receive mandatory training on:
    - How to recognize and report security incidents.
    - What to expect during the incident response process.
- Specialized training is given to:
    - CSIRT members
    - DevOps teams
    - Project managers with high-risk client deliverables

“Security is a moving target. Our response process evolves with every incident, every lesson, and every technological advancement.”

Vulnerability Management Policy

1. Introduction & Purpose

At **Live Now Technology SLU**, we recognize that vulnerabilities in software, infrastructure, and third-party dependencies pose a **critical risk** to our operations, client trust, and regulatory compliance. As a company that develops and manages digital systems in high-integrity environments — including Earth observation data processing, scientific software, and system engineering — it is our responsibility to maintain a **proactive and disciplined approach** to vulnerability management.

This policy establishes a comprehensive framework for:

- Identifying, evaluating, prioritizing, and mitigating security vulnerabilities across all systems and environments.
- Maintaining compliance with best practices and security standards such as **ISO/IEC 27001**, **OWASP**, **NIST SP 800-40**, and **ENISA guidance**.
- Minimizing the attack surface and ensuring the integrity, availability, and confidentiality of services.

The purpose of this document is to:

- Prevent exploitation of known vulnerabilities in our assets and codebases.
- Maintain real-time visibility into exposure to technical and logical flaws.
- Promote a secure-by-design development lifecycle and patching process.
- Align with internal risk management, information security, and quality assurance practices.

2. Scope & Applicability

This policy applies to:

- All digital assets owned, operated, or managed by **Live Now Technology SLU**, including:

  - Web applications, APIs, backend services, and mobile platforms.
  - Internal systems (e.g., mail, cloud storage, project management tools).
  - Cloud environments, CI/CD pipelines, databases, and source code repositories.
  - Third-party services, libraries, and vendor integrations.
- All personnel involved in:
  - Software development
  - DevOps / system administration
  - Security and compliance
  - Project and technical management
- All stages of the asset lifecycle:
  - Design and development
  - Deployment and maintenance
  - Legacy and sunset systems

Vulnerability management is required across **production, staging, and development environments**, and includes both **custom code** and **third-party dependencies**.

3. Objectives of the Vulnerability Management Program

The core objectives of this program are to:

3.1 Proactively Identify Vulnerabilities

- Implement automated and manual tools to detect known security flaws.
- Monitor vulnerability databases, threat intelligence feeds, and vendor advisories (e.g., CVE, NVD, GitHub Advisories, vendor-specific alerts).
- Integrate scanning into the SDLC and infrastructure lifecycle.

3.2 Prioritize Risk-Based Remediation

- Classify vulnerabilities based on **technical severity, exploitability, business impact, and asset criticality**.

- Focus efforts on fixing issues with **highest risk** first (e.g., CVSS ≥ 7, exploitable remotely, affecting client-facing services).

- Track exposure time and ensure **timely resolution** against predefined SLAs.

3.3 Maintain Compliance and Best Practice Alignment

- Ensure adherence to security controls required under:
    - **ISO 27001 / Annex A.12.6.1** (technical vulnerability management)
    - **NIS2**, **GDPR** (data protection)
    - **Client-specific contractual obligations**

- Be prepared for **audits and external assessments** by maintaining detailed logs and vulnerability reports.

3.4 Foster Security Awareness and Collaboration

- Educate developers, DevOps, and stakeholders on secure coding, dependency hygiene, and vulnerability implications.

- Encourage a security-first mindset and collaboration between security and delivery teams.

4. Vulnerability Identification (Sources & Tools)

Vulnerabilities must be detected as early as possible using a combination of **automated scanning**, **manual review**, and **intelligence sources**.

4.1 Scanning and Monitoring Tools

- **Static Application Security Testing (SAST)**: Integrated into the CI/CD pipeline to identify code-level issues during development.
- **Dynamic Application Security Testing (DAST)**: Periodic scans of deployed applications to identify runtime vulnerabilities.
- **Dependency Scanning**: Tools like **npm audit**, **yarn audit**, **pip-audit**, or **OWASP Dependency-Check** to identify vulnerable packages.
- **Infrastructure Scanning**: Tools such as **Tenable**, **Qualys**, or **OpenVAS** used on cloud infrastructure, containers, and VMs.
- **Cloud Security Posture Management (CSPM)**: Monitoring tools (e.g., AWS Security Hub, GCP Security Command Center) to detect misconfigurations or public exposure.

4.2 External Intelligence Feeds

- Public databases: **CVE**, **NVD**, **ExploitDB**, **GitHub Security Advisories**.
- Vendor-specific advisories (e.g., from Microsoft, Atlassian, AWS, GitLab).
- CERTs (e.g., **INCIBE-CERT**, **ENISA**, **CERT-EU**).
- Participation in **industry-specific threat intelligence groups** where applicable.

4.3 Manual Discovery & Penetration Testing

- Scheduled **internal penetration tests** or **bug bounty simulations**.
- Secure code reviews during peer-review processes.
- Third-party penetration tests as required by clients or audits.

5. Risk Classification & Prioritization

Not all vulnerabilities pose the same risk. **Live Now Technology SLU** follows a risk-based prioritization approach using industry-standard scoring and context-specific analysis.

5.1 Severity Classification

Severity is initially determined using the **Common Vulnerability Scoring System (CVSS v3.x):**

CVSS Score	Severity Level
9.0 – 10.0	cal
7.0 – 8.9	
4.0 – 6.9	ium
0.1 – 3.9	

Additional contextual factors considered:

- **Exploitability** (public PoC, active exploitation in the wild)
- **Data sensitivity** (PII, client assets)
- **Business criticality** of affected system
- **Network exposure** (public vs internal)

5.2 Remediation SLAs

Severity	Time to Remediate
Critical	hours
High	business days
Medium	days
Low	esources permit

Deviations from these timelines require **formal risk acceptance** by the Information Security Officer.

6. Remediation and Mitigation Process

6.1 Remediation Workflow

1. **Detection**: Vulnerability is identified via automated scan or manual input.
2. **Verification**: Technical lead or security analyst confirms the finding is valid and non-false-positive.
3. **Prioritization**: Severity and impact are evaluated using risk classification matrix.
4. **Ticketing**: Issue is logged in the company’s issue tracker with metadata (CVSS, CWE, impacted system).
5. **Assignment**: Owner/team responsible is assigned with SLA and deadline.
6. **Remediation**: Patch, configuration change, or code fix is implemented.
7. **Testing**: Change is tested in a safe environment.
8. **Closure**: Issue is marked as resolved, and logs are retained.

6.2 Mitigation Strategies

If immediate remediation is not possible:

- **Network segmentation or access restriction** is enforced.
- **Web Application Firewall (WAF)** rules are updated to block exploitation.
- **Monitoring alerts** are configured to detect abuse attempts.
- **Communication to stakeholders** is issued if exposure is client-facing.

6.3 Tracking and Documentation

- All vulnerabilities are tracked in a central **Vulnerability Register** with:
    - Detection date, remediation status, responsible team, residual risk.
- KPIs (e.g., average remediation time, SLA compliance rate) are reviewed monthly.

7. Patch Management and Third-Party Dependencies

Keeping software components, systems, and third-party libraries **up-to-date** is a critical pillar of the vulnerability management strategy.

7.1 Patch Management Process

- **Patches are applied based on severity and criticality**, according to the SLAs defined in Section 5.
- All **production systems** are included in the patching schedule.
- Changes are tested in **staging environments** before being deployed to production to avoid regressions.
- Emergency patching protocols are in place for **zero-day vulnerabilities** (e.g., Log4Shell, Heartbleed).
- Monthly patching windows are maintained for standard updates across internal infrastructure.

7.2 Third-Party Software and Dependencies

- Software projects must use **dependency management tools** (e.g., npm, pip, Maven) with automated security checks.
- Regular updates of third-party libraries are enforced through CI pipelines.
- All external libraries must have:

  - Clear versioning and changelogs.
  - Licenses reviewed by the legal or compliance team (where applicable).
  - Security advisories actively monitored.

7.3 Unsupported and End-of-Life Software

- Systems or packages that are no longer supported by the vendor must be:
  - **Decommissioned** or replaced.
  - **Isolated** in segmented environments.
  - Subject to additional monitoring and compensating controls.

8. Monitoring, Metrics & Continuous Improvement

To ensure the effectiveness of the vulnerability management program, **Live Now Technology SLU** tracks key indicators and performs ongoing process reviews.

8.1 Key Performance Indicators (KPIs)

- Number of vulnerabilities detected (per category/severity).
- Mean time to remediate (MTTR).
- SLA compliance rate by severity.
- Percentage of assets scanned regularly.
- Dependency update frequency in active projects.

8.2 Monitoring Tools and Dashboards

- Centralized dashboards (e.g., through Jira, GitHub, or custom monitoring) track remediation workflows.
- Alerts are configured for overdue items or unresolved critical issues.
- Weekly or monthly reports are reviewed by the **Security and Engineering Leads**.

8.3 Continuous Improvement

- Lessons learned from security incidents are fed back into:
  - Development processes (e.g., secure coding practices).
  - Infrastructure reviews (e.g., tightening IAM, firewall rules).
  - CI/CD pipelines (e.g., improved checks or automation).
- Process adjustments are made after:
  - New threat landscape shifts.
  - Vulnerability exploitation trends.
  - Regulatory or contractual changes.

9. Roles, Responsibilities & Governance

9.1 Security Lead / CISO (or Designated Officer)

- Oversees the entire vulnerability management program.
- Approves risk acceptance justifications and tracks residual risks.
- Leads the selection and deployment of scanning tools.
- Reports regularly to executive management.

9.2 DevOps & Engineering Teams

- Implement patches, configuration changes, and mitigation actions.
- Integrate security scanning into the software development lifecycle (SDLC).
- Maintain updated dependency files and avoid deprecated versions.

9.3 Project Managers & Product Owners

- Prioritize remediation work during sprints or maintenance cycles.
- Communicate to clients if their environments or deliverables are impacted.
- Align remediation efforts with contractual or regulatory obligations.

9.4 All Employees

- Stay informed about security hygiene best practices.
- Promptly report unusual behavior or suspected vulnerabilities.
- Avoid the use of unapproved or outdated software packages.

9.5 Audits and Reviews

- Annual internal audits assess process adherence.
- The policy is reviewed **at least once per year**, or after any major incident or vulnerability event.
- Results are communicated to the management team and included in compliance documentation.

> *“Vulnerability management is a shared responsibility — everyone in the organization contributes to a secure and trusted environment.”*

Internal Employee Communication Channel

1. Purpose and Commitment

Live Now Technology SLU is committed to maintaining a workplace culture based on **transparency, ethics, and accountability**. To support this, we provide an **internal and confidential reporting mechanism** for employees, contractors, and collaborators to **report misconduct, policy violations, or risks** anonymously or openly.

We strictly enforce a **no-retaliation policy** for all good-faith reports.

2. Scope of Reportable Issues

This mechanism covers, but is not limited to:

- Ethical misconduct (e.g., discrimination, harassment, conflict of interest)
- Financial irregularities (e.g., fraud, corruption, embezzlement)
- Breaches of security, data protection, or company policies
- Violations of law, contracts, or regulatory obligations

3. How to Report

Employees, collaborators, and external partners may report incidents or concerns using the company's **designated internal reporting channel**, designed to ensure **confidentiality, accessibility, and compliance** with EU and Spanish whistleblowing laws.

3.1 Reporting Methods:

- **Secure Online Form**: Accessible from the intranet or internal portal, available 24/7. It allows both identified and anonymous submissions.
- **Dedicated Email Address**: (e.g., `report@livenowtech.com`) configured with restricted access and encryption.
- **Optional Phone Contact**: For sensitive or urgent matters, a secure voicemail system may also be provided.
- **Written Reports**: Can be submitted directly to the Compliance Officer in a sealed envelope marked “Confidential – Ethics Report”.

3.2 Report Contents Should Include (if known or applicable):

- A clear description of the event, issue, or misconduct.
- Date and location of occurrence.
- Parties involved or affected.
- Any evidence or supporting documents.
- Contact information (optional, if anonymity is not requested).

No personal details are required for anonymous reporting. The system will not collect IP addresses or other identifiable metadata.

4. Handling and Follow-Up

Once a report is submitted, **Live Now Technology SLU** follows a standardized, compliant investigation process to ensure fairness and confidentiality.

4.1 Report Intake and Logging

- All reports are received by the **Ethics & Compliance Officer** or a specifically designated person (not involved in the facts).

- Each report is logged with a unique ID and timestamped in a secure register (digital or physical).

4.2 Initial Assessment

- Within **7 calendar days**, an initial triage is completed to:
    - Confirm receipt to the whistleblower (if identified).
    - Determine whether the report falls within the policy's scope.
    - Decide if immediate actions are required (e.g., prevent further harm).

4.3. Investigation Process

- If admissible, a confidential internal investigation is launched.
- The process includes fact-finding interviews, documentation review, and expert consultation where necessary.
- Investigations are concluded within **a maximum of 90 days**, extendable in complex cases (as per EU Directive).

4.4 Follow-Up Communication

- If the whistleblower has provided contact information, they will receive updates:
    - Confirmation of receipt.
    - General progress (without revealing sensitive or legal details).
    - Final outcome or resolution status.

5. Protection and Confidentiality

We ensure a **safe environment for speaking up**. No one will be penalized or discriminated against for making a good-faith report.

5.1 Non-Retaliation Guarantee

- Retaliation (e.g., dismissal, demotion, harassment) against any person who submits a report in good faith is strictly prohibited.
- Confirmed retaliation will result in **disciplinary actions up to termination**.

5.2 Anonymous Reporting Protection

- Anonymous reports are fully accepted and processed equally.
- The reporting system is configured to **not log metadata, IPs, or user details**.
- Anonymous submitters may use tracking codes to check their case status (if supported by the system).

5.3 Confidentiality Measures

- All information is handled under **strict confidentiality**.
- Only authorized personnel directly involved in the investigation have access to the report.
- Disclosures are limited to what is legally required or necessary for resolution.

> *“Raising concerns strengthens our organization — and those who do so deserve absolute protection.”*

Equality Polices

To foster a transparent and ethical work culture, this policy introduces the public mechanisms related to the equality and fairness of the Company.

Criteria for access to employment

The applicant entity declares its firm commitment to equal treatment and equal opportunities between women and men in all selection processes and access to employment, in accordance with the provisions of:

- Ley orgánica 3/2007 del 22 de Marzo 2007, for the effective equality of women and men.
- Real Decreto 901/2020, on equality plans and their registration.
- Real Decreto 902/2020, on equal pay for women and men.

And other applicable regulations on non-discrimination in the workplace.
In compliance with said regulations, and aligned with the principles of the extended RIS3 Strategy, the company will implement the following specific and verifiable measures within the framework of the project:

- Inclusive and neutral wording of offers. All job offers linked to the project will be written in inclusive language, avoiding gender stereotypes, and clearly specifying that it is a work environment committed to equality.

Example of a clause: "This company applies active equal opportunity policies. Applications will be considered regardless of sex, gender identity, sexual orientation, origin, religion or family situation".

Equal distribution in different channels. The offers will be published in:

- Generalist platforms (InfoJobs, LinkedIn).
- Specific channels that promote equality and diversity, including job boards of women technologist associations or female talent networks. This aims to achieve a critical mass of applications from both sexes.

Assessment based exclusively on objective competencies. During the selection process:
Pre-defined and published assessment criteria (hard & soft skills) will be established.
Standardized assessment tools (technical tests, comparative matrices) will be used to minimize unconscious bias.

Questions unrelated to professional performance, such as those related to family life, future maternity or unreasonable time availability, will be eliminated.
Previously defined and published assessment criteria will be established (hard & soft skills).
Standardized assessment tools (technical tests, comparative matrices) will be used to minimize unconscious bias.

Questions unrelated to professional performance, such as those related to family life, future maternity or unreasonable time availability, will be eliminated.

Mandatory equality training for personnel with recruitment functions. The team responsible for selection and recruitment will receive mandatory training on:

- Legal framework for equality and non-discrimination.
- Unconscious biases and gender stereotypes.
- Best practices in equal opportunities in selection processes.

Registration and traceability of processes. All contracting processes related to the project will be documented with:

- Offer publications.
- Lists of candidates.
- Scoring matrices.
- Minutes or records of interviews.

This guarantees verifiability in the event of any control or audit, and makes it possible to identify possible gaps for correction.

Monitoring indicators. During the development of the project the following KPIs will be monitored:

- % of applications received by gender.
- % of pre-selected and hired persons by gender.
- Comparison between results and staff composition.

These indicators will be part of the internal quality and continuous improvement system.
In summary, access to the jobs related to the subsidized project will be governed by the principles of merit, capacity, objectivity, real equality and transparency, in accordance with Spanish labor legislation and Community guidelines on gender equality.

Promotion criteria

Our company promotes a work environment based on merit, professional competence and the principle of effective equality between women and men, in accordance with the provisions of Article 45 of Organic Law 3/2007, as well as Royal Decree 901/2020, which establishes the obligation of objective and transparent criteria in professional promotion, especially in companies benefiting from public aid.

During the implementation of the subsidized project and in general in the corporate culture, the following specific measures will be applied to ensure that internal promotion processes are carried out without gender bias or direct or indirect discrimination:
Advertising of internal opportunities. All opportunities for promotion or professional improvement linked to the project (such as promotions, assignment of tasks of responsibility, expansion of functions or access to higher-level technical positions) will be communicated internally and publicly to the entire workforce, guaranteeing:
Equal access to information.
Reasonable times for the presentation of candidacies.
Direct communication channels such as corporate mailing.
Prior and objective definition of promotion criteria. The objective requirements for access to

each promotion process will be established and communicated in advance, which may include:

Accredited technical experience.

Performance evaluation in the current position.

Participation in key projects.

Relevant technical training or specific skills.

These criteria will be aligned with the profiles required in the subsidized project and will be common to all staff, without distinction based on gender, age or other non-professional personal characteristics.

Documentary record and traceability. All promotion decisions will be documented and incorporated into internal personnel management and compliance systems. This includes:

Lists of interested persons.

Benchmarking results.

Objective reasons for selection of the promoted person.

This traceability will allow, if required, to demonstrate that the promotion has been based exclusively on transparent and non-discriminatory professional criteria.

Monitoring indicators. To ensure continuous improvement in equality, the following indicators will be monitored and analyzed periodically:

Percentage of promotions made by gender.

Evolution of female participation in positions of responsibility.

Comparison between the percentage of women in the workforce and the percentage of women promoted.

If unjustified inequalities are detected, corrective measures will be activated within the framework of the HR policy review.

In short, the company undertakes to guarantee effective equality of opportunities for professional development for all the people who make up the team, including those directly linked to the subsidized project. Internal promotion is governed by the principles of objectivity, transparency, merit, capacity and co-responsibility.

Remuneration systems and criteria that comply with the parameters of publicity, objectivity and transparency and promote the principle of equality and non-discrimination.

The company assumes the firm commitment to guarantee that the remuneration policy applied to all employees, and especially to those who participate in the development of the subsidized project, rigorously complies with the principles of equal pay, transparency, objectivity and non-discrimination based on sex or any other personal or social condition, in accordance with the provisions of Royal Decree 902/2020, on equal pay between women and men, and ley orgánica 3/2007.

The company's remuneration structure is based on a model by salary levels and bands defined according to the value of the position, with no link to the person occupying it. Salary conditions are established on the basis of technical criteria, responsibility, qualifications and professional experience, and are applicable homogeneously to people performing equivalent functions.

In order to ensure the correct implementation of this model, the following measures are adopted:

Remuneration transparency. All employees have access to the company's general salary band structure through internal documentation, and the economic conditions are expressly communicated in writing at the time of hiring or in any review process. In the case of people linked to the subsidized project, they will be provided with all the information related to the remuneration system that affects them.

Remuneration register. The company prepares and updates annually a remuneration register disaggregated by sex, in accordance with Article 5 of Real Decreto 902/2020. This register includes:

Total annual remuneration (salary and supplementary).

Percentage differences by sex, category and position.

Objective reasons for possible differences (if any), justified by documents.

This record will be available to the legal representation of workers or, failing that, to the labor inspectorate in case of requirement.

Objective performance evaluation. Variable remuneration complements or incentives that may be received by personnel linked to the project will be based exclusively on the fulfillment of clearly defined objectives or indicators, and never on subjective elements that cannot be evaluated.

Corrective measures in the event of an unjustified pay gap. In the event that, through the analysis of the pay register, differences that are not objectively justified are detected, the company undertakes to:

Carry out a diagnostic report.

Adopt a corrective plan with defined deadlines and specific measures.

Document and communicate the actions taken to the workforce.

Verifiability of the system before control bodies. All remuneration elements of the personnel linked to the project will be clearly traceable, justified and accessible for any review by the public administration, thus ensuring compliance with the principle of transparency in the use of public funds.

Implementation of specific measures to prevent sexual harassment and gender-based harassment at work (codes of conduct, action protocols, etc.).

The company has adopted a set of specific measures aimed at preventing, detecting and acting against situations of sexual or gender-based harassment in the workplace, in compliance with the provisions of Artículo 48 de la Ley Orgánica 3/2007, which requires all companies, regardless of their size, to have specific procedures for this purpose.

These measures are integrated within the company's general policy of equality and good practices, which can be found on its website, and are articulated as follows:

Harassment prevention and action protocol. The company has a specific protocol for the prevention and action in cases of sexual harassment and harassment based on sex, which has been approved, disseminated and signed by management. This protocol establishes

Clear and specific definition of conduct constituting harassment.

Confidential channels for filing complaints or internal communications.

Guaranteed investigation procedure with defined deadlines.

Precautionary measures during the process, if necessary.

Applicable sanctions and redress mechanisms.

The protocol is available on the internal employee portal and on the corporate website, and is also provided to new recruits as part of the onboarding program.

Code of conduct with a gender perspective. The company has approved a professional code of conduct that establishes rules for coexistence at work and principles of responsible behavior, including explicit clauses against gender-based violence or discrimination.

This code is part of the organization's ethical and integrity framework, and is integrated as a reference document in all internal HR processes, including those linked to the subsidized project.

Training and awareness-raising. The workforce receives regular training and awareness-raising activities on equality, respect, prevention of harassment and non-sexist communication.

This training:

It is mandatory for all management personnel and team leaders.

It is included in the initial onboarding for new hires.

It is updated according to regulatory developments or best practices.

Explicit commitment in the company's culture. Management promotes an organizational culture based on zero tolerance of harassment and violence in the workplace, reflected in:

Periodic internal communications.

Contractual documentation and internal regulations.

Public positioning of the company as an inclusive and safe organization.

Verifiability before audit or inspection. All documents (protocol, training provided, minutes, internal communications) are archived and available to the competent bodies, as part of the commitment to responsible management of public aid and effective compliance with the legal framework.

Adoption of measures in the companies to promote the presence of women on boards of directors, in other collegiate bodies and in the rest of the different decision-making positions and their evolution in recent years.

The company is aware of the structural imbalance that has historically existed in terms of the representation of women in decision-making positions, especially in the technology sector. Therefore, it assumes as a strategic priority to actively promote the balanced participation of women and men in collegiate bodies, management teams and positions with leadership and decision-making capacity, both at the current level and in future growth.

In this sense, the following specific measures have been adopted, appropriate to the size and evolution of the company:

Formal commitment to parity in the governance structure. The commitment to effective equality is manifested in the corporate governance structure itself, where the objective of achieving and maintaining a gender balance in collegiate bodies, technical decision-making committees and project management has been established as a guiding principle.

In phases of expansion, the principle of substantive equality will be applied so that the incorporations to management bodies prioritize female representation in technical and strategic positions, especially in traditionally male-dominated areas such as engineering, software development or systems management.

Internal promotion of female talent to positions of responsibility. The company actively encourages the career progression of female staff members, especially to positions with leadership capabilities. This includes:

Identification of internal female talent with leadership potential.

Preferential inclusion in team management, project management or negotiation training.

Periodic internal evaluation of professional growth opportunities from an equity perspective.

Inclusion of the principle of balanced representation in future expansions. In view of the implementation of the subsidized project, and as part of the growth plan foreseen in Phase II of the business model, any new decision-making body, advisory board or strategic committee created must respect a balanced composition, in accordance with the definition contained in Organic Law 3/2007 (minimum of 40% representation of each sex, whenever possible).

Monitoring and evolution of indicators. There will be an internal follow-up that allows monitoring the presence of women in:

Decision-making bodies.

Project coordination.

High-level technical teams.

Positions of responsibility or external representation functions.

This system makes it possible to evaluate the evolution over time, detect possible gaps and design corrective measures if necessary.

With this set of measures, the company seeks not only to comply with current legislation, but also to promote a structural and permanent change towards a more balanced, representative and diverse leadership model, especially relevant in the digital and innovation sector.