Company Policies and Procedures

Preamble

At GeniaDynamics, we are committed to creating a positive and productive work environment that fosters collaboration, innovation, and respect. Our policies and procedures are designed to promote fairness, equity, and inclusion, while also ensuring compliance with applicable laws and regulations. This document outlines our internal regulations and guidelines for employees, contractors, and visitors. It is intended to provide a framework for responsible behavior and decision-making, and to help ensure that everyone associated with our company conducts themselves in a manner that reflects our values and principles.

Section 0. Definitions

- **Company** - refers to GeniaDynamics, a software development company, and its subsidiaries, affiliates, and branches.
- **Employee** - refers to any individual working for the Company, including full-time employees, part-time employees, contractors, interns, and temporary workers.
- **Management** - refers to the Company's management team, including managers, supervisors, and team leads.
- **Workplace** - refers to any location where work is performed, including offices, remote work locations, or client sites.
- **Confidential Information** - refers to any information that is not publicly available and is considered sensitive or proprietary, such as trade secrets, business strategies, customer data, and employee personal information.
- **Intellectual Property** - refers to any intellectual property rights, including patents, copyrights, trademarks, and trade secrets, owned or licensed by the Company.
- **IT Resources** - refers to any computer systems, software applications, networks, and other technology resources provided by the Company for employee use.
- **Work Hours** - refers to the standard hours of work established by Management, which may vary depending on the role and department.

- **Break Periods** - refers to the designated times during the workday when employees are entitled to take breaks.
- **Personal Devices** - refers to any personal electronic devices brought into the workplace, such as smartphones, tablets, or laptops.

Section 1. Employee conduct and ethics

At GeniaDynamics, we believe that maintaining high ethical standards is essential to our success. We expect all employees to adhere to the highest levels of professionalism, honesty, and integrity in their interactions with colleagues, customers, suppliers, and other stakeholders.

The following are some guidelines for employee conduct and ethics:

- **1.1. Honesty and Integrity**
  - Be truthful and transparent in all your dealings, both inside and outside the company.
  - Avoid any behavior that could be perceived as dishonest or unethical.
  - Refrain from engaging in any activity that could compromise your integrity or the integrity of the company.
- **1.2 Respect for Colleagues**
  - Treat all colleagues with respect and dignity, regardless of their position or background.
  - Avoid discrimination, harassment, or bullying of any kind.
  - Foster an inclusive work environment where everyone feels valued and welcome.
- **1.3 Confidentiality**
  - Maintain the confidentiality of company information and data at all times.
  - Do not share sensitive information with unauthorized individuals or entities.
  - Refrain from discussing company business in public areas or on social media platforms.
- **1.4 Compliance with Laws and Regulations**
  - Familiarize yourself with relevant laws, regulations, and industry standards that apply to your role.
  - Ensure that all your actions comply with these requirements.
  - Report any potential violations of law or ethical standards to your supervisor or HR immediately.
- **1.5 Gifts and Entertainment**

  - Avoid accepting gifts or entertainment from suppliers, customers, or other stakeholders if they could be seen as influencing your business decisions.
  - Ensure that any gifts or entertainment you receive are modest in value and not linked to a specific business transaction.

- **1.6 Conflict of Interest**
  - Avoid situations where your personal interests conflict with the interests of the company.
  - Disclose any potential conflicts of interest to your supervisor or HR immediately.

- **1.7 Social Media Conduct**
  - Refrain from posting anything on social media that could damage the reputation of the company or its employees.
  - Avoid sharing confidential information or engaging in discussions that could be perceived as inappropriate or offensive.

- **1.8 Reporting Ethical Violations**
  - If you witness or suspect a violation of ethical standards, report it to your supervisor, HR, or the anonymous ethics hotline immediately.
  - The company will investigate all reports promptly and take appropriate action.

- **1.9 Compliance Training**
  - Attend all mandatory compliance training sessions to ensure you are aware of the latest laws, regulations, and industry standards that apply to your role.

Disciplinary actions:

Our company may have to take disciplinary action against employees who repeatedly or intentionally fail to follow our code of conduct. Disciplinary actions will vary depending on the violation, possible consequences include:

- Demotion.
- Reprimand.
- Suspension or termination for more serious offenses.
- Detraction of benefits for a definite or indefinite time.
- We may take legal action in cases of corruption, theft, embezzlement or other unlawful behavior.

By adhering to these guidelines, we can maintain a workplace culture that is built on trust, respect, and integrity. We expect all employees to embrace these principles and help us uphold the highest ethical standards at all times.

Section 2. Compliance with laws and regulations

The organization is committed to complying with all applicable laws and regulations in the European Union, including but not limited to the General Data Protection Regulation (GDPR), the EU's data protection law. We recognize the importance of protecting personal data and ensuring that it is handled in accordance with relevant laws and regulations.

To ensure compliance, we have implemented a number of measures, including:

2.1 Data Protection Impact Assessment (DPIA)

We conduct regular DPIAs to identify, assess, and mitigate any potential privacy risks associated with our processing of personal data.

2.2 Privacy by Design

We have implemented a 'privacy by design' approach to ensure that data protection is integrated into the development of all our products and services from the outset. This means that we consider data protection when designing new systems, processes, and technologies, and strive to minimize the amount of personal data we collect and process.

2.3 Data Protection Policy

We have developed a comprehensive Data Protection Policy that sets out our approach to protecting personal data. The policy covers topics such as data security, data retention, and data subject rights. All employees are required to read and comply with the policy.

2.4 Training

We provide regular training for all employees on data protection laws and regulations, as well as our own Data Protection Policy. This includes training on GDPR, data classification, data security, and incident response.

2.5 Incident Response Plan

We have developed an Incident Response Plan that sets out the steps we will take in case of a data breach or other security incident. The plan ensures that we are able to respond quickly and effectively to any incidents that may occur.

2.6 Data protection Agreements

We ensure that all our vendors, suppliers, and sub-processors who handle personal data have signed data protection agreements with us. These agreements require them to comply with GDPR and other relevant laws and regulations.

2.7 Cross-Border Data Transfer

We have implemented appropriate safeguards for cross-border data transfers in accordance with the European Commission's Standard Contractual Clauses (SCCs) and Privacy Shield Framework, where applicable.

2.8 Data Subject Rights

We respect the rights of individuals under GDPR, including their right to access, rectify, erase, restrict processing, object to processing, and data portability. Individuals may exercise these rights by contacting our DPO.

2.9 Regular Review

We regularly review and update our policies, procedures, and training programs to ensure they remain compliant with the latest laws and regulations.

2.10 Commitment

By implementing these measures, we demonstrate our commitment to protecting personal data in accordance with applicable laws and regulations in the European Union.

Section 3. Intellectual property protection

GeniaDynamics recognizes the importance of protecting its intellectual property, including patents, trademarks, copyrights, trade secrets, and confidential information. This section outlines our policy and procedures for protecting and enforcing our intellectual property rights.

3.1 Ownership of Intellectual Property

GeniaDynamics retains ownership of all intellectual property rights arising from work performed by employees, contractors, or agents in the course of their employment or engagement with GeniaDynamics. This includes any inventions, discoveries, creations, or other works that are developed using company resources or time.

3.2 Protection of Intellectual Property

GeniaDynamics is committed to protecting its intellectual property from unauthorized use, disclosure, or exploitation. To achieve this, we implement appropriate security measures such as access controls, encryption, and confidentiality agreements. We also monitor our intellectual property rights and take legal action when necessary to enforce them.

3.3 Use of Intellectual Property

Employees, contractors, and agents are prohibited from using GeniaDynamics's intellectual property for personal gain or in any way that may harm the company's interests. Any use of our intellectual property must be authorized by the appropriate manager and in accordance with our policies and procedures.

3.4 Disclosure of Intellectual Property

Employees, contractors, and agents are prohibited from disclosing GeniaDynamics's intellectual property to any third party without prior authorization from the appropriate manager. This includes but is not limited to trade secrets, confidential information, or other proprietary data.

3.5 Enforcement of Intellectual Property Rights

GeniaDynamics will take all necessary steps to enforce its intellectual property rights in case of any violation or infringement. This may include legal action, injunctions, damages, or any other remedy available under law.

3.6 Compliance with Laws and Regulations

GeniaDynamics complies with all applicable laws and regulations related to intellectual property protection. We also expect our employees, contractors, and agents to comply with these laws and regulations when working on behalf of the company.

3.7 Review and Revision

This policy will be reviewed and revised periodically as necessary to ensure that it remains effective and relevant. Any changes will be communicated promptly to all employees, contractors, and agents who have access to GeniaDynamics's intellectual property.

By following this policy, we can protect our intellectual property rights and prevent unauthorized use or disclosure of our proprietary information. It is the responsibility of every employee, contractor, and agent working for GeniaDynamics to adhere to these policies and procedures.

Section 4. Data security and privacy

GeniaDynamics takes the protection of our customers, employees, and partners personal information very seriously. We are committed to ensuring that all data collected, stored, or processed by us is protected from unauthorized access, disclosure, modification, or destruction. This section outlines our policies and procedures for protecting sensitive information.

4.1 Responsibilities

- All employees, contractors, consultants, temporary workers, interns, and other personnel who have access to sensitive data are responsible for following this policy.
- The IT department is responsible for implementing security measures to protect our systems and networks from unauthorized access.
- Data owners are responsible for identifying and classifying the types of data they handle and ensuring that appropriate security controls are in place.

Data category	**Definition**	**Security Controls**
public	Information that is intended for public consumption or access. Examples include our website, press releases, and marketing materials.	backed-up regularly, integrity verification.
internal	Information that is intended for internal use only but does not contain sensitive information. Examples include employee contact lists, meeting notes, and company announcements.	Access controls, encryption when transmitted or stored, backed-up regularly, Hashing.
confidential	Information that contains personally identifiable information (PII), financial data, intellectual property, or other highly sensitive information. Examples include customer records, employee personal data, and business strategy documents.	Strong access controls, encryption both in transit and at rest, secure storage, backed-up regularly, Hashing.

Table 1: Data security classification

- All personnel who handle sensitive data must use strong passwords, keep them confidential, and follow best practices for password management.

4.2 Data Classification

We classify our data into three categories based on its level of sensitivity: public, internal, and confidential. Table 4.1 defines each category and outlines the appropriate security controls for each one.

4.3 Data Security Measures

We implement the following security measures to protect our systems and networks from unauthorized access:

- Firewalls and intrusion detection/prevention systems (IDPS) to monitor network traffic for suspicious activity.
- Secure authentication, authorization, and accounting (AAA) protocols for all users accessing our systems.
- Encryption of sensitive data both in transit and at rest.
- Access controls, including secure login credentials, two-factor authentication, and role-based access control (RBAC).
- Secure protocols for remote access to our systems, such as virtual private networks (VPNs) and or secure shell (SSH).

- Regular software updates and patches to ensure that all systems are current with the latest security fixes.
- Logging and monitoring of system activity to detect potential security breaches.
- Regular security testing and vulnerability assessments to identify and remediate potential weaknesses.

4.4 Data Breach Response

In the event of a data breach, we will follow our incident response plan to minimize the damage and protect affected individuals' personal information. The plan includes the following steps:

- Containment: Isolate affected systems or networks to prevent further unauthorized access.
- Assessment: Identify the scope of the breach, including what data was accessed and how many individuals were affected.
- Notification: Inform affected individuals and regulatory agencies as required by law.
- Eradication: Remove any malware or unauthorized access points from our systems.
- Recovery: Restore systems to a secure state, including patching vulnerabilities and resetting passwords.
- Lessons Learned: Document the breach and response for future reference and improvement.

4.5 Data Retention and Disposal

We retain personal information only as long as necessary to fulfill the purpose for which it was collected or as required by law. When we no longer need the data, we dispose of it securely using one of the following methods:

- Paper documents are shredded or recycled.
- Electronic files are deleted and overwritten with random characters to prevent recovery.
- Media devices such as hard drives or USB sticks are physically destroyed or degaussed.

4.6 Training and Compliance

All employees must complete annual training on data security and privacy best practices. The training covers topics such as password management, social engineering

attacks, phishing scams, and safe browsing habits. Additionally, all personnel who handle sensitive data must sign a confidentiality agreement acknowledging their responsibility to protect it. We monitor compliance with this policy and take disciplinary action when necessary.

4.7 Third-Party Vendors

We evaluate third-party vendors' security practices before engaging in business relationships or sharing personal information. Vendors must demonstrate that they have implemented appropriate security controls to protect our data. We monitor vendor compliance with their agreed-upon security measures and conduct regular audits to ensure continued adherence.

4.8 Compliance

We comply with all applicable laws and regulations regarding data privacy, including but not limited to the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Payment Card Industry Data Security Standard (PCI DSS). We also adhere to industry standards such as ISO 27001 for information security management.

4.9 Conclusion

Data security and privacy are critical components of our business operations, and we take all necessary measures to protect sensitive information from unauthorized access or disclosure. This policy outlines our procedures for handling personal data and ensures that we comply with legal requirements while maintaining the trust of our customers, employees, and partners.

Section 5. Quality assurance

GeniaDynamics is committed to providing high-quality products and services that meet or exceed our customers' expectations. In order to achieve this goal, we have implemented a comprehensive quality assurance program that includes the following elements:

5.1 Quality Objectives

We have established clear and measurable quality objectives for all of our products and services. These objectives are reviewed and updated regularly to ensure they remain relevant and achievable.

5.2 Quality Management System

We operate a quality management system that is compliant with ISO 9001:2015, the international standard for quality management systems. This system provides a framework for managing our processes, procedures, and resources to ensure we consistently meet customer requirements and regulatory obligations.

5.3 Continuous Improvement

We believe in continuous improvement and strive for excellence in all aspects of our business. We regularly review our processes and procedures to identify opportunities for improvement and implement changes as needed.

5.4 Customer Feedback

We value feedback from our customers and use it as an opportunity to improve our products and services. We have a formal process for collecting, analyzing, and responding to customer feedback, which helps us make informed decisions about product development and quality improvements.

5.5 Document Control

We maintain strict control over all documents related to our products and services, including product specifications, quality manuals, and procedures. We ensure that only the latest versions of these documents are used, and we have a formal process for updating and approving changes.

5.6 Continuity and Business Resilience

We recognize that unexpected events can impact our ability to deliver high-quality products and services. Therefore, we have developed business continuity plans and risk management strategies to ensure our operations continue uninterrupted in the event of an emergency or disaster.

By following these quality assurance procedures, GeniaDynamics is committed to providing its customers with safe, reliable, and high-quality products and services that meet their expectations and comply with all relevant regulations.

Section 6. Project management

The purpose of this policy is to establish guidelines for effective project management within the organization, ensuring that projects are delivered on time, within budget, and to the required quality standards.

6.1 Scope

This policy applies to all projects undertaken by the organization, regardless of their size or complexity. It covers the entire project lifecycle, from planning and execution to monitoring and control, and finally, to closure.

6.2 Roles and Responsibilities

a) Project Manager: The Project Manager is responsible for leading and coordinating the project team, ensuring that projects are delivered within the agreed-upon timeframe, budget, and quality standards. They will also be responsible for managing

stakeholder expectations, identifying and mitigating risks, and communicating project progress to relevant parties.

b) Project Team: The Project Team consists of all individuals involved in the project, including team members, contractors, and consultants. They are responsible for carrying out their assigned tasks and responsibilities as directed by the Project Manager.

c) Stakeholders: Stakeholders include anyone who has an interest in or will be impacted by the project. They may include customers, sponsors, management, and other relevant parties.

6.3 Project Planning

a) Project Charter: The Project Charter is a document that outlines the purpose, objectives, scope, timelines, budget, and stakeholders of the project. It provides authorization for the project to proceed and serves as a reference point throughout the project lifecycle.

b) Work Breakdown Structure (WBS): The WBS is a hierarchical decomposition of the project into smaller, manageable tasks that can be scheduled and budgeted for. It helps to define the scope of work and ensures that all tasks are accounted for.

c) Project Schedule: The project schedule outlines the start and end dates for all tasks and milestones, as well as any dependencies between them. It provides a roadmap for the project team to follow and helps ensure that the project is completed on time.

d) Budgeting: The budgeting process involves estimating costs for resources required for the project, including labor, materials, equipment, and other expenses. The budget should be comprehensive, taking into account contingencies and risks.

e) Risk Management: A risk management plan should be developed to identify potential risks that may impact the project. This includes assessing their likelihood and impact, as well as developing strategies for mitigation or response.

6.4 Project Execution

a) Task Assignment: The Project Manager will assign tasks to team members based on their strengths, expertise, and availability. Team members are expected to carry out their assigned tasks in accordance with the project schedule and quality standards.

b) Quality Control: Quality control measures should be implemented throughout the project lifecycle to ensure that deliverables meet the required standards. This includes inspections, testing, and other quality assurance activities.

c) Communication Plan: A communication plan should be developed to ensure effective communication among all stakeholders. It should outline the types of communication, frequency, channels, and key messages.

d) Change Management: Any changes to the project scope, schedule, budget, or quality must be formally documented and approved by the Project Manager and relevant stakeholders. This includes assessing the impact of the change on the project

and obtaining agreement from all affected parties.

6.5 Monitoring and Control

a) Progress Reporting: Regular progress reports should be submitted to the Project Manager, highlighting accomplishments, issues, and future tasks. These reports help monitor project status and identify any deviations from the plan.

b) Performance Metrics: Key performance metrics (KPIs) should be established to measure project success. These may include schedule performance index, cost performance index, quality metrics, and customer satisfaction surveys.

c) Corrective Actions: If project progress or performance indicates deviations from the plan, corrective actions must be taken promptly to get the project back on track. This may involve revising task assignments, adjusting timelines, or reallocating resources.

6.6 Closure

a) Finalization of Deliverables: All deliverables should be finalized and reviewed by the Project Manager and stakeholders to ensure they meet quality standards.

b) Documentation: The project documentation should be completed and updated, including lessons learned, which can be used for future projects.

c) Evaluation: A post-project evaluation should be conducted to assess project success, identify areas for improvement, and document best practices for future reference.

d) Celebration: The project team should celebrate the successful completion of the project, recognizing individual contributions and achievements.

By following these guidelines, our organization can ensure that projects are delivered efficiently, effectively, and to a high standard, ultimately contributing to our business success.

Section 7. Communication and collaboration

Effective communication and collaboration are critical components of our company's success. In this section, we outline the policies and procedures for internal and external communication, as well as strategies for effective teamwork and collaboration.

7.1 Internal Communication

Our company encourages open and transparent communication among all team members. We believe that clear and timely communication helps to build trust, resolve conflicts, and promote a positive work environment. To ensure effective internal communication, we adopt the following practices:

Regular team meetings: We hold regular team meetings to discuss project updates, share information, and address any concerns or issues.

Open-door policy: Our team members are encouraged to approach their supervisors or HR with questions, concerns, or feedback at any time.

Internal communication channels: We use a private instance of NextCloud Hub for internal communication. All team members are expected to check these channels regularly and respond promptly to messages.

7.2 External Communication

We recognize that effective external communication is essential for building strong relationships with our clients, partners, and stakeholders. Our company adopts the following policies for external communication:

Client communication: We communicate with our clients through email. We ensure that all communications are professional, courteous, and respectful.

Media relations: Our company's media relations policy aims to build and maintain positive relationships with the press and other media outlets. We respond promptly to media inquiries and ensure that our messaging is consistent and aligned with our brand values.

Crisis communication: In the event of a crisis, we have a crisis communication plan in place to manage external communications effectively. The plan includes procedures for issue identification, containment, eradication, recovery, and post-crisis evaluation.

7.3 Collaboration

Collaboration is critical to our company's success. We believe that by working together, we can achieve better results than individually. Our collaboration policies aim to foster a culture of teamwork, respect, and open communication. The following are some strategies we use to promote collaboration:

Cross-functional teams: We create cross-functional teams to encourage collaboration among different departments and functions.

Collaboration tools: We use Nextcloud Hub and gitlab to facilitate collaboration among team members.

Feedback culture: Our company encourages a feedback culture where team members can provide constructive feedback to each other to improve our work processes and outcomes.

7.4 Confidentiality and Data Protection

Our company respects the privacy of our clients' and partners' information. We adopt strict confidentiality and data protection policies to ensure that sensitive information is handled appropriately. All team members are expected to sign a non-disclosure agreement (NDA) before starting work with our company. We also comply with relevant data protection regulations, such as the General Data Protection Regulation (GDPR).

7.5 Language and Communication Style

Our company recognizes that language and communication style can impact how we collaborate and communicate effectively. We adopt the following policies to ensure clarity and inclusivity in our communication:

Language: Our official language is English. However, we recognize that our team members may speak different languages, and we encourage them to communicate in their native language if needed.

Communication style: We promote a respectful and professional communication style. We avoid using jargon or technical terms that may confuse or intimidate others. Our communication should be clear, concise, and appropriate for our audience.

Section 8. Employee training and development

At GeniaDynamics, we recognize the importance of investing in our employees' growth and development. Our goal is to provide opportunities for personal and professional growth, as well as to foster a culture of continuous learning and improvement. To achieve this, we offer various training programs and initiatives that cater to different roles and career paths within the organization.

8.1 Training Programs:

We offer a range of training programs designed to enhance technical, managerial, and soft skills. These include but are not limited to:

- Technical training for software development, testing, and maintenance;
- Leadership and management training for supervisors and managers;
- Communication, teamwork, and collaboration training;
- Time management, prioritization, and productivity training;
- Customer service and sales training;

8.2 Training Methods:

We understand that different individuals have different learning styles, so we offer a variety of training methods to cater to these differences. These include but are not limited to:

- Instructor-led classroom training;
- Online courses and webinars;
- On-the-job training;
- Mentoring programs;

- Self-paced learning modules;

8.3 Career Development:

We believe in promoting from within, and we encourage our employees to pursue their career goals within the company. To support this, we offer career development opportunities such as job rotations, cross-functional projects, and mentorship programs. Our aim is to help employees acquire new skills, gain valuable experience, and advance in their careers.

8.4 Performance Management:

We have a performance management system that includes regular feedback, goal setting, and performance evaluations. This system helps us identify areas where employees need improvement and provide them with the necessary training and support to excel in their roles. Our performance management process also allows us to recognize and reward outstanding performance.

8.5 Employee Engagement:

We believe that engaged employees are more productive, motivated, and committed to achieving our company's goals. To foster engagement, we encourage open communication, provide opportunities for employee feedback, and offer recognition programs to appreciate our employees' hard work and dedication. Our aim is to create a positive work environment where employees feel valued, respected, and empowered to make a difference.

8.6 Continuous Improvement:

We continuously review and update our training programs and policies to ensure they remain relevant and effective. We welcome feedback from employees and management on ways to improve our training initiatives and employee development opportunities. Our goal is to create a culture of continuous learning, improvement, and growth that benefits both the company and our employees.

Section 9. Workplace safety

We are committed to providing a safe and healthy work environment for all employees. The following guidelines have been established to ensure that our workplace is free from hazards and risks associated with physical, psychological, or ergonomic factors. It is the responsibility of every employee to adhere to these guidelines and report any concerns or incidents promptly to their supervisor or HR department.

9.1 Physical Safety

a) All employees must wear appropriate attire, including safety shoes, goggles, gloves, and hard hats when working in areas where potential hazards exist (e.g., construction sites, production floors).

b) Employees are prohibited from engaging in horseplay or other dangerous behavior that could put themselves or others at risk of injury.

c) The company will provide ergonomic furniture and equipment to minimize the risk of musculoskeletal disorders. Employees must report any discomfort or pain associated with their workstation to their supervisor or HR department for assistance.

d) Fire extinguishers, first aid kits, and emergency exit routes will be inspected regularly and maintained in good working condition. Emergency drills will be conducted quarterly to ensure that all employees are familiar with evacuation procedures.

9.2 Psychological Safety

a) The company is committed to maintaining a workplace free from harassment, discrimination, or bullying of any kind. Employees must treat each other with respect and dignity at all times. Any instances of inappropriate behavior will be investigated promptly and addressed according to our disciplinary procedures.

b) The company recognizes that mental health is just as important as physical safety. We encourage employees to take breaks, practice stress-reducing techniques, or seek professional help when needed. Confidential counseling services are available upon request through our employee assistance program (EAP).

9.3 Remote Work Safety

a) Employees working from home or other remote locations must ensure their workspace meets basic safety standards, including proper lighting, ergonomic furniture, and a secure internet connection.

b) Remote employees are expected to maintain regular working hours and take breaks as needed to avoid fatigue and burnout. They should also inform their supervisor or HR department of any changes in their work environment that may impact their productivity or well-being.

9.4 Incident Reporting

a) All incidents, including accidents, injuries, property damage, or security breaches, must be reported to the employee's supervisor or HR department immediately. An incident report form will be provided for this purpose and must include details of what happened, when, where, who was involved, and any recommended actions to prevent future occurrences.

b) The company will investigate all incidents promptly and take appropriate action to address the root cause(s). Employees may also provide feedback or suggestions on how to improve workplace safety through our intranet portal or during regular team meetings.

9.5 Safety Training

a) New employees will receive mandatory safety training as part of their onboarding process, which includes reviewing this policy document and attending a workplace

safety orientation session conducted by HR or the designated safety officer.

b) Regular safety training sessions and workshops will be provided for all employees to refresh their knowledge and skills in areas such as first aid, fire prevention, cybersecurity awareness, and stress management.

9.6 Contractors and Visitors

a) All contractors and visitors must adhere to our workplace safety policies when on company premises or working on company projects. They will be required to sign a copy of this policy document before starting work and attend a safety orientation session if necessary.

b) The company reserves the right to deny access to any individual who fails to comply with our safety policies or poses a risk to themselves or others.

Section 10. Group's Constitution

The group number two of LESI (Licenciatura em Engenharia de Sistemas Informáticos) is made up of the following members:

- Diogo Antunes
- Edgar Baptista
- João Ribeiro
- José Senra

The group's advisor is the esteemed teacher Patrícia Isabel Sousa Trindade Silva Leite, who can participate in the group's meetings to help the conception of the project's objectives.

Section 11. Positions and how often they rotate

The positions on the company are mainly static, changes occur only upon written notice of the executive board

Engineering positions:

Team lead -	Diogo Antunes (effective)
Software Developer/Engineer -	Diogo Antunes (effective) João Ribeiro (effective) Edgar Baptista (effective) José Senra (effective)
Software/Solutions Architect -	Diogo Antunes (effective) Edgar Baptista (effective)
Quality Assurance (QA) Engineer -	Diogo Antunes (effective) Edgar Baptista (effective)
Database Administrator (DBA) -	Diogo Antunes (effective) João Ribeiro (effective)
System Administrator -	Diogo Antunes (effective) João Ribeiro (effective)
UX/UI Designer -	João Ribeiro (effective)
Systems Analyst -	Diogo Antunes (effective) Edgar Baptista (effective)
Scrum Master -	João Ribeiro (effective)
DevOps engineer	Diogo Antunes (effective) Edgar Baptista (effective)
Product Manager -	João Ribeiro (effective)
Project Manager	Diogo Antunes (effective)
Data Scientist	Diogo Antunes (effective)
Data Protection Officer (DPO) -	Diogo Antunes (effective)
Cybersecurity Engineer -	Diogo Antunes (effective)
Technical writer	José Senra (effective)

Executive positions

Chief Executive Officer (CEO) -	Diogo Bernardo
Chief Operating Officer (COO) -	Edgar Baptista
Chief Financial Officer (CFO) -	João Ribeiro
Chief Technology Officer (CTO) -	Diogo Bernardo
Chief Information Officer (CIO) -	José Senra
Chief Human Resources Officer (CHRO) -	João Ribeiro
Chief Legal Officer (CLO) -	Diogo Bernardo