Information Security Policy

1. Contents

2. Information security management system policy and objectives

At Exponam, we are committed to ensuring the confidentiality, integrity, and availability of information within our scope of software development, systems integration, computer programming consultancy, and related activities. This policy establishes the framework for our information security management system (ISMS) to protect our assets and meet the requirements of ISO/IEC 27001:2022. It is the ISMS of Exponam that information, as defined hereinafter, in all its forms - written, spoken, recorded electronically, or printed – will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

This policy will be communicated to all employees, contractors, and relevant stakeholders. It will be made available to interested parties upon request.

This policy will be reviewed annually or as needed to ensure its continuing suitability, adequacy, and effectiveness.

3. Information security management system objectives

These general objectives provide a comprehensive framework for building and maintaining an effective ISMS. They serve as a foundation upon which specific security controls and measures can be implemented to address the unique risks and requirements of an organization.

Our primary information security objectives are:

● Confidentiality: To ensure that sensitive information is accessible only to authorized individuals.

● Integrity: To safeguard the accuracy and completeness of information and processing methods.

● Availability: To ensure that information and information processing facilities are available when needed.

We are committed to complying with all applicable legal and regulatory requirements related to information security in the jurisdiction where we operate.

We will conduct regular risk assessments to identify, evaluate, and prioritize information security risks. Appropriate controls will be implemented to mitigate these risks to an acceptable level. Roles and responsibilities for information security will be defined, communicated, and documented. All employees, contractors, and third-party entities with access to our information assets will be made aware of their responsibilities.

We will provide ongoing training and awareness programs to ensure that all employees and relevant stakeholders are aware of information security risks, policies, and procedures.

Access to information and information processing facilities will be controlled based on business requirements and the principle of least privilege. Access rights will be reviewed and updated regularly. We will integrate security measures into the software development and systems integration processes, including secure coding practices, vulnerability assessments, and penetration testing.

We will establish and maintain procedures for reporting, assessing, and responding to information security incidents. Lessons learned will be used to improve our security posture.

We will monitor the effectiveness of our ISMS through regular performance measurement, internal audits, and management reviews.

We are committed to continually improving our ISMS to adapt to changing business needs, emerging threats, and technological advancements.

4. Information security management system manual

This section describes in more detail document scope, context of the organization, information security management system structure, roles and responsibilities and normative references.

Scope

The scope of ISMS includes information security to protect the confidentiality, integrity, and availability of information.

ISMS in the scope of this document is meant as a compilation of all the various policies which are included in the document as well as referencing to all separate external full-bodied sections to manage information security in accordance with ISO/IEC 27001:2022. It stands for establishing, implementing, maintaining and continually improving ISMS, so it is up to date, is in accordance with organization and its context, as well as interested parties - is corresponding with actual business plans or needs and is fully integrated into the processes and business activities of the organization.

ISMS documentation describes how data, assets and security is managed and secured, how employees are trained, who is responsible for what information, processes and procedures, how this documentation is continually updated and approved with management to keep an ever-evolving ISMS and be able to respond to all new emerging threats and vulnerabilities.

The framework for managing information security described in this document applies to all Exponam involved persons and all involved systems throughout Exponam.

This policy and all standards apply to all protected health information and other classes of protected information in any form as defined in 6.2.2. Information classification policy.

The scope of the Information Security Management System (ISMS) encompasses the provision of services in the areas of Software Development, Systems Integration, Computer Programming Consultancy, and related activities. This includes all processes, technologies, and personnel associated with these services within our organization.

This scope is defined to ensure the confidentiality, integrity, and availability of sensitive information, both belonging to our organization and entrusted to us by our clients and stakeholders. By establishing and maintaining a robust ISMS, we aim to safeguard the interests of all parties involved and uphold the highest standards of information security.

The context of the organization

- **Company background:**

Exponam was founded in 2017 to solve problems with modern data via innovative software solutions. The company is based in New Hampshire with operations in Portsmouth NH and New York.

- **Interested Parties and Their Relevant Requirements:**

  - **Clients/Customer Organizations**

Relevant Requirements:

Clients almost always have individual requirements additionally to any available standards, therefore Exponam ISMS policies are prepared in a modular way, linked to ISMS as external documents - to be able to deliver just the required separate policy or procedure not the whole documentation.

Addressed through ISMS:

Implementation of robust access controls, encryption, and secure coding practices.

Adherence to industry-specific security standards (e.g., ISO 27001).

○ **Regulatory Authorities**

Relevant Requirements:

Compliance with applicable data protection and privacy laws.

Reporting of security incidents and breaches.

Addressed through ISMS:

Regular risk assessments and compliance audits.

Incident response and reporting procedures.

○ **Legal Counsel**

Relevant Requirements:

Adherence to contractual obligations and legal requirements.

Addressed through ISMS:

Clearly defined policies and procedures aligned with legal and contractual obligations.

Regular legal review to ensure compliance.

○ **Employees and Contractors**

Relevant Requirements:

Awareness and training on security policies and procedures.

Access to information necessary for their role.

Addressed through ISMS:

Employee awareness and training programs.

Role-based access controls and regular access reviews.

○ **Third-Party Vendors and Suppliers**

Relevant Requirements:

Security of shared data and information.

Adherence to security standards and practices.

Addressed through ISMS:

Vendor risk assessments and due diligence.

Contractual clauses define security expectations.

○ **Internal Stakeholders (Management, Board of Directors)**

Relevant Requirements:

Assurance of information security practices.

Oversight of compliance and risk management.

Addressed through ISMS:

Regular reporting and communication on ISMS effectiveness.

Executive support and allocation of resources for ISMS.

○ **Industry Partners and Associations**

Relevant Requirements:

Adherence to industry-specific security standards and best practices.

Addressed through ISMS:

Active participation in industry forums and compliance with industry standards.

Information security management system structure

The organization of information security is the foundational structure and framework put in place within Exponam to proficiently manage all aspects of information security practices. This comprehensive system ensures that sensitive information is handled with the utmost care and in compliance with industry-leading standards.

● Information Security Management System (ISMS):

At Exponam, we have established an all-encompassing Information Security Management System (ISMS) that is meticulously designed, implemented, maintained, and continuously improved in strict adherence to the latest ISO/IEC 27001:2022 standards. This internationally recognized framework serves as the backbone of our information security practices, providing a robust structure for safeguarding sensitive data.

● Enhancing Accessibility and Oversight:

This centralized approach significantly enhances accessibility, allowing authorized personnel to swiftly locate and refer to pertinent policies. Moreover, it facilitates greater oversight, enabling us to monitor adherence to established policies and promptly address any deviations or emerging risks.

● Strengthening ISMS Effectiveness:

By leveraging this centralized document control system, we fortify the effectiveness of our ISMS. It streamlines processes, minimizes the risk of information security breaches, and fosters a culture of security awareness and compliance across the organization.

● Continuous Improvement:

Our commitment to information security extends beyond implementation. We are dedicated to an ongoing cycle of evaluation, enhancement, and refinement of our ISMS, ensuring that it remains at the forefront of industry best practices.

Roles and responsibilities

Exponam has defined the following Information security related roles and responsibilities.

Top management:

Role: This includes the organization's executives and senior leaders who have the ultimate responsibility for the ISMS.

Responsibilities:

Demonstrating leadership and commitment to information security (Clause 5.1).

Establishing the information security policy and objectives (Clause 5.2).

Providing the necessary resources for the ISMS (Clause 7.1).

Information security manager:

Role: The information security manager oversees the development, implementation, and maintenance of the ISMS.

Responsibilities:

Coordinating and managing the ISMS implementation (Clause 6.2).

Ensuring compliance with ISO/IEC 27001 requirements (Clause 4.3).

Conducting risk assessments and defining security controls (Clause 6.1).

The ISM or ISO for each entity is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of Exponam. Specific responsibilities include:

● Ensuring security policies, procedures, and standards are in place and adhered to by entity.

● Providing basic security support for all systems and users.

● Advising owners in the identification and classification of computer resources. See Section VI Information Classification.

● Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.

● Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.

● Providing on-going employee security education.

● Performing security audits.

● Reporting regularly to the Exponam Oversight Committee on the entity's status regarding information security.

Risk manager:

Role: The risk manager is responsible for identifying, assessing, and managing risks to information assets.

Responsibilities:

Conducting regular risk assessments and vulnerability scans (Clause 6.1.2).

Identifying potential threats and vulnerabilities (Clause 6.1.3).

Recommending and implementing risk mitigation measures (Clause 6.1.3).

Information asset owners:

Role: Information asset owners are responsible for specific information assets within the organization.

Responsibilities:

Determining the classification and labeling of information assets (Clause 7.2).

Defining access controls and permissions for their respective assets (Clause 7.2).

Ensuring compliance with security policies and controls (Clause 7.2).

The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the Exponam Information Owner Delegation Form. The owner of information has the responsibility for:

● Knowing the information for which she/he is responsible.

● Determining a data retention period for the information, relying on advice from the legal department.

● Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.

● Authorizing access and assigning custodianship.

● Specifying controls and communicating the control requirements to the custodian and users of the information.

● Reporting promptly to the information security manager the loss or misuse of Exponam Information.

● Initiating corrective actions when problems are identified.

● Promoting employee education and awareness by utilizing programs approved by the ISM, where appropriate.

● Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

System administrators:

Role: System administrators manage and maintain information systems and networks.
Responsibilities:

Implementing and enforcing security controls on systems and networks (Clause 8.1).

Conducting regular system audits and vulnerability assessments (Clause 8.1).

Ensuring the timely application of security patches and updates (Clause 8.1).

Internal auditors:

Role: Internal auditors are responsible for conducting periodic audits to assess the effectiveness of the ISMS.

Responsibilities:

Planning and conducting internal audits of the ISMS (Clause 9.2).

Reporting audit findings and recommending corrective actions (Clause 9.2).

Monitoring the implementation of corrective actions (Clause 9.2).

User managers

Exponam management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

● Reviewing and approving all requests for their employees’ access authorizations.

● Initiating security change requests to keep employees' security record current with their positions and job functions.

● Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.

● Revoking physical access to terminated employees, i.e., confiscating keys, keycards, changing combination locks, etc.

● Providing employees with the opportunity for training needed to properly use the computer systems.

● Reporting promptly to the ISO the loss or misuse of Exponam information.

● Initiating corrective actions when problems are identified.

● Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

Employees and users:

Role: All employees and users within the organization have a role to play in maintaining information security.

Responsibilities:

Following security policies and procedures (Clause 7.3).

Reporting security incidents or vulnerabilities promptly (Clause 10.1).

Participating in security awareness and training programs (Clause 7.2).

The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

● Access information only in support of their authorized job responsibilities.

● Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.

● Keep personal authentication devices (e.g. passwords, SecureCards, PINs, etc.) confidential.

● Report promptly to the ISO the loss or misuse of Exponam information.

● Initiate corrective actions when problems are identified.

Compliance Manager:

Role: The compliance manager ensures that the organization adheres to all relevant legal and regulatory requirements related to information security.

Responsibilities:

Monitoring changes in regulations and standards (Clause 4.2).

Ensuring that the ISMS remains compliant with ISO/IEC 27001 (Clause 4.3).

Coordinating with legal and regulatory bodies as necessary (Clause 4.2).

Normative references

1. ISO/IEC 27001:2022 - Information security, cybersecurity, and privacy protection -Information security management system - Requirements.

2. ISO/IEC 27000:2018 - Information Technology - Security Techniques - Information security management system - overview and vocabulary

3. ISO/IEC 27002:2022 - Information security, cybersecurity, and privacy protection -Information security controls

4. ISO/IEC 27003:2017 - Information technology security techniques Information security management systems guidance

5. ISO/IEC 27004:2016 - Information technology security techniques Information security management monitoring, measurement, analysis and evaluation

6. ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection - Guidance on managing information security risks

7. ISO 31000:2018 - Risk management guidelines

8. ISO/IEC 27001:2002 - Annex A Controls

Definitions, terms and abbreviations

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.
Availability: Data or information is accessible and usable upon demand by an authorized person.
Involved persons: Every worker at Exponam – no matter what their status. This includes residents, students, employees, contractors, consultants, temporary workers, volunteers, interns, etc.

Involved systems: All computer equipment and network systems that are operated within the Exponam environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in house or licensed from third parties) contained on those systems.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.
Information resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand held computers, personal digital assistants (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed,

built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information technology support and security (ITSS): Exponam IT department responsible for information and technology security, computers, networking and data management.

Entity: Every separate Exponam company and location, team and department.

ISP: Information security policy.

ISO: Information security officer.

ISM, CISO: Information security manager or chief information security officer.

IT: Information technology.

ISMS: Information security management system.

Company: Exponam

AWS: Amazon web services

MFA: Multi factor authentication

OTP: One time password

5. Risk management

● Risk assessment and treatment methodology: Describe the approach to identifying, evaluating, and treating risks.

● Risk Register: Maintain a record of identified risks, their assessments, and treatment plans. ● Risk Treatment Plans: Provide specific details on how each identified risk will be addressed.

Information security risk management

● A comprehensive risk assessment of all Exponam information networks and systems will be conducted at least annually or when significant changes occur within the organization, to identify and document the threats and vulnerabilities to stored and transmitted information. This process will also include a business impact analysis to determine the potential impact of various threats on critical business functions.

● The risk assessment will analyze various types of threats – internal or external, natural or manmade, electronic and non-electronic – that may affect the confidentiality, integrity, and availability of information resources. The assessment will also evaluate the information assets and the technology associated with their collection, storage, dissemination, and protection, considering the specific requirements and compliance obligations for financial institutions.

● The risk assessment will document the existing vulnerabilities within each entity, which potentially expose the information resource to identified threats. Based on the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the information's confidentiality, integrity, and availability will be determined.

● The frequency of the risk assessments will be determined at the entity level, with a minimum requirement of an annual assessment or when significant changes occur within the organization.

● Based on the risk assessment outcomes, appropriate risk mitigation measures will be implemented to reduce the impact of the threats by decreasing the amount and scope of the vulnerabilities. Risk mitigation strategies may include technical, administrative, and physical controls.

● Exponam will establish risk acceptance criteria to define the acceptable level of risk. Any risks exceeding the defined risk acceptance criteria will be escalated to the appropriate management level for review and decision-making.

● Regular monitoring and review of the effectiveness of implemented risk mitigation measures will be conducted to ensure that they remain relevant and effective in addressing the identified risks. The results of this monitoring will be reported to the ISO and other relevant stakeholders. Risk management processes will be aligned with industry best practices, such as the NIST Cybersecurity Framework and ISO/IEC 27001, and will be subject to regular reviews and updates to ensure continuous improvement and adaptability to the evolving threat landscape.

Risk register and treatment plan

Risk register and treatment plan is described in Exponam corporate risk log in this external document - refer to: "**Corporate risk log**", available to the Risk Management.

Risk is identified and added to the risk log as described in 4.3. **- Corporate risk management**.

Corporate risk management

As the Company recognizes the importance of a structured approach to corporate risk management and internal control, this policy is put in place to provide the framework to identify, assess, monitor, and manage risks associated with the Company's business.

Corporate Risk Management Policy has been described in this external document - refer to: "**P030 Corporate Risk Management Policy**".

Business continuity management

The purpose of this business continuity plan is to prepare Exponam in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. All Exponam Consulting sites are expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when a n incident occurs.

The plan identifies vulnerabilities and recommends necessary measures to prevent extended voice communications service outages. It is a plan that encompasses all Exponam sites and operations facilities.

Business Continuity Management has been described in this external document - refer to: "**P011 Business Continuity and Disaster Recovery plan".**

Important aspect of risk management is ISMS itself - are processes and responsibilities unclear or is there poor engagement of the top management or poor awareness of employees about IS or its purpose, insufficient documentation or in contrary too detailed or complicated.

Also opportunities should be identified, for example cooperation with other companies regarding IS or using ISMS to make changes in the company to achieve other benefits like enhanced productivity or employee engagement.

Regarding all identified risks, the company should plan actions to avoid them and integrate those actions into processes of the ISMS and evaluate how effective those actions are.

Statement of applicability

Statement of applicability and implementation status of ISO/IEC 27001:2022 Annex A controls has been described in this external document - refer to: "**Statement of applicability"**, available to Risk Management.

6. Control procedures and policies

Access control policy

Physical and electronic access, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access for internal workers, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by Exponam. Mechanisms to control access, Confidential and Internal information include (but are not limited to) the following methods:

Authorization

Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

- **Context-based access**

Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.

- **Role-based access**

An alternative to traditional access control models (e.g., discretionary or non

discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

- **User-based access**

A security mechanism used to grant users of a system access based upon the identity of the user.

Identification and authentication

Unique user identification (user id) and authentication is required for all systems that maintain or access Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

At least one of the following authentication methods must be implemented:

- strictly controlled passwords (5.1.10. - **Password Policy**),
- biometric identification, and/or
- tokens in conjunction with a PIN.

The user must secure his/her authentication control (e.g., password, token) such that it is known only to that user and possibly a designated security manager.

An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes).

The user must log off or secure the system when leaving it.

MFA is mandatory for all systems where that is available. Google platform MFA setup and use is explained in this external document - refer to: "**20230525_Google Platform MFA setup and user guide_v1**".

Data integrity

Exponam must be able to provide corroboration that Confidential and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

- transaction audit
- checksums (file integrity)
- encryption of data in storage
- digital signatures

Transmission security

Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

integrity controls and encryption, where deemed appropriate.

Remote access (BYOD and teleworking policy)

Access into Exponam network from outside will be granted using Exponam approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protection as information stored and accessed within the Exponam network.

The purpose of this policy is to establish guidelines for employees who utilize their own devices to work or bring them to work at the company office to ensure the security and confidentiality of company data.

This policy applies to all employees who utilize their own devices to work.

● Employees are allowed to bring their own devices to work, including smartphones, tablets, and laptops.

● It is not permitted to connect personally owned equipment to any network socket at the work office. Personally owned devices should use the wireless network.

● Employees must not store any company information assets on their personal devices unless authorized by the company or by signing remote work agreements or specified by the license agreement. Company may require adding such devices to AppleSeeds instance to partially manage Apple devices.

● Whenever possible, information asset storage must be provided by company cloud services, rather than stored on individual computers locally. If that is not possible, then the user is responsible also for information asset accessibility and integrity ensuring data backup procedures are in place.

● Employees must ensure information asset integrity, whenever synchronization between Employees and Company takes place, to ensure that the most current, uncorrupted information or data is available.

● Information and data separation must be ensured between work and personal use by using separate folders or user accounts.

● Employees must not share their devices with others, including family members or friends.

● Employees must not download or install any unauthorized software or applications on their devices.

● Employees must report any lost or stolen devices to the Information Services immediately.

● Employees must understand and comply with all company policies and procedures related to data security and confidentiality, as well as Information Classification and Information Asset use.

● Employees are responsible for security and confidentiality regarding company data and information assets and must perform actions that prevent unauthorized persons accessing that data and information.

● Employees must ensure that their devices are password protected and have up-to date antivirus software installed.

● It is required to lock access to the computer when the Employee is away from it by using screen-lock, signing-out or shutting down the computer.

Physical access

Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

File servers containing Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:

● Position workstations to minimize unauthorized viewing of protected health information.

● Grant workstation access only to those who need it in order to perform their job function.

● Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected health information.

● Use automatic screen savers with passwords to protect unattended machines.

Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

● Contingency Operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

● Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

● Access Control and Validation – Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

● Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

Additional physical security policy has been described in this external document - refer to: "**P014 Physical Security Policy".** Physical access instruction has been described in this external document - refer to: "**Physical Access instructions_06012020**".

Emergency access

Each entity is required to establish a mechanism to provide emergency access to systems and applications if the assigned custodian or owner is unavailable during an emergency.

Procedures must be documented to address:

● Authorization

● Implementation

● Revocation

If not stated otherwise by an individual, then by a chain of command PM or higher manager may become a temporary owner during an emergency, however ISO or ISM should be notified to properly record this as a probable security incident.

Access control review

Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges by the System Administrator. Examples of accounts with excessive privileges include:

An active account assigned to external contractors, vendors or employees that no longer work for the Institution.

An active account with access rights for which the user's role and responsibilities do not require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system. System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator. Unknown active accounts.

User access management policy

The purpose of this policy is to prevent unauthorized access to the Exponam's information systems. The policy describes the registration and de-registration process for all Exponam information systems and services.

User Access Management Policy has been described in this external document - refer to: **"P019 User Access Management Policy"**.

Password policy

Password complexity, as well as password change, password confidentiality and other password requirement details are explained in this external document - refer to: **"P019 User Access Management Policy"**.

Encryption and cryptography

These terms are used in AWS to secure virtual hosts and when signing with a secure signature (signature usage is mandatory in the company and enforced through the onboarding process when hiring a new employee). Google Workspace uses the latest cryptographic standards to encrypt all data at rest and in transit between its facilities. In addition, Gmail uses TLS (Transport Layer Security) for communication with other email service providers. With Gmail Client-side encryption (CSE), you can strengthen the confidentiality of your sensitive or regulated data content by having the encryption handled in your browser before any data is transmitted or stored in Google's cloud-based storage. This provides uniform protection to your messages until it is received by the intended recipients. Also encryption may be used to securely transfer or store data offline (e.g. archiving with a password), but as cloud services offer more secure and easy to use services, that becomes obsolete. Bitlocker is enabled when configuring new laptops for employees. Encryption should be used in development (e.g. to secure a publicly accessible database).

IT asset classification and handling policy

Information assets

All involved systems and information are assets of Exponam and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

- **Ownership of information assets**

All computer software developed by Exponam employees or contract personnel on behalf of Exponam or licensed for Exponam use is the property of Exponam and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

The storage, transmission, distribution or use of copyrighted material not legally owned by or licensed to the user, or the company is strictly prohibited on Exponam computers (or individually owned computers in case of BYOD/Teleworking) and networks. This includes, but is not limited to, movies, photos, music, and other copyrighted content. Furthermore, any non-work-related data should not be stored on company systems to maintain the security and integrity of information assets

- **Installed software**

All software packages that reside on computers and networks within Exponam must comply with applicable licensing agreements and restrictions and must comply with Exponam acquisition of software policies.

Information classification policy

Exponam provides fast, efficient, and cost-effective electronic services for a variety of clients worldwide.

It is critical for Exponam to set the standard for the protection of information assets from unauthorized access, compromise, and disclosure. Accordingly, Exponam has adopted this information classification policy to help manage and protect its information assets.

Information Classification Policy has been described in this external document - refer to: "**P012 Information Classification Policy"**.

IT assets

This policy is designed to protect the organizational resources on the network by establishing a policy and procedure for IT asset control. These policies will help prevent the loss of data or organizational assets and will reduce the risk of losing data.

IT Asset Control and Disposal policy has been described in this external document - refer to: "**P016 Asset Control and Disposal policy**, explaining asset types, tracking, transfer, and disposal procedures.

Acceptable information technology infrastructure and resource use policy

This policy outlines acceptable use of IT resources (which includes, but is not limited to software, hardware, and networks) and infrastructure by any individuals working at Exponam. Acceptable Information Technology Infrastructure, Resource Use Policy has been described in this external document - refer to: "**P017 Acceptable Information Technology Infrastructure _ Resource Use Policy"**.

Information security incident management

The purpose of this policy is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. It enables the efficient and effective management of incidents by providing a definition of an incident and establishing an overall structure for the reporting and management of such incidents.

Information Security Incident Management has been described in this external document - refer to: "**P018 Information Security Incident Management Policy"**.

Physical and environmental security

Physical and environmental security is a section of the information security policy that addresses measures to protect the organization's physical assets and infrastructure. It includes guidelines for the secure management and use of facilities, equipment, and other physical resources. The policy may cover areas such as access control, monitoring, and protection against environmental threats like fire

and water damage. It may also outline procedures for secure disposal of sensitive information and equipment. The goal of this section is to ensure that the physical environment is secure and that the organization's assets are protected against unauthorized access, theft, or damage.

Physical and environmental security aspects have been described in this external document - refer to: "**P014 Physical Security Policy"**.

Clean desk and screen policy

Staff with access to sensitive information are responsible for ensuring that information is always controlled and/or protected by taking appropriate actions to prevent loss, theft, misuse, or unintended disclosure of this information in their workspace (i.e. offices, cubicles, residential and work-at-home environments, hotels, conference centers, and public spaces). These actions include, but are not limited to:

● Sensitive information in any format or media must be securely stored (i.e., locked cabinet or drawer) when not in use.

● All sensitive information must promptly be removed from unattended or non-secured areas (e.g. conference rooms and break rooms), printers, fax machines, and incoming mail points. Any items left in these areas for an extended time must be securely disposed of.

● Unauthorized duplication or reproduction of sensitive information is specifically prohibited. This includes but is not limited to photocopying, scanning, and photography.

● Staff must set their workstation to a password protected screen saver any time it is unattended (for example, using Ctrl+Alt+Delete buttons and selecting "Lock this Computer" or by using the Windows Key + L).

● Desktop screensaver lock must also be set to automatically launch after no more than 15 minutes of inactivity.

● VPN tokens or other similar user authentication mechanisms must be safeguarded when not in use or when unattended.

● If a work area is visible from a less restricted area (e.g. exterior windows), users should attempt to configure the work area such that computer screens are not easily visible from the less restricted area.

● Staff must exercise caution when sharing/displaying computer screens via web meetings or desktop sharing technologies with external parties. In such instances, staff must only share the information adequate for the purpose of the call, and only grant permission to see the information to those who have a genuine business need.

● Media handling and data transfer management

● Secure system development and maintenance

● System monitoring and logging

- Backup
- Incident management and response
- Supply chain security

By implementing operational security measures, organizations can mitigate risks associated with the day-to-day operation of their information systems and ensure that their data is secure and available when needed.

E-mail policy

All use of email must be consistent with Exponam policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

Exponam email account should be used primarily for Exponam business related purposes and personal communication is permitted on a limited basis using a reasonable amount of Exponam resources (non-work-related email shall be saved in a separate folder), but non-Exponam related commercial uses are prohibited.

Sending chain letters or joke emails from a Exponam email account is prohibited.

The Exponam email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Exponam employee should report the matter to their supervisor immediately.

Users are prohibited from automatically forwarding Exponam email to a third-party email system. Individual messages which are forwarded by the user must not contain Exponam confidential or above information.

Exponam employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Exponam may monitor messages without prior notice. Exponam is not obliged to monitor email messages.

Exponam email should not be registered with any external service provider, if that is not related to work and work responsibilities.

Virus protection

Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

Backup policy

The backup is a crucial component of information security that ensures the availability and integrity of data in case of data loss or system failure. This section should address the backup strategy, including frequency, retention period, and storage location. The backup policy should specify the backup procedures, such as the type of backups, media used, and the backup schedule. Additionally, the policy should outline the procedures for testing the backup system to ensure its effectiveness and include a plan for disaster recovery. Finally, the backup section should outline the roles and responsibilities of staff involved in the backup process and specify the security measures to protect the backup data.

Google Drive and Microsoft Disc are available to all users of the company and may be used to backup critical information. Automatic backup procedures as well as additional backup solutions may be implemented if necessary to better improve the integrity and availability of information stored.

The company uses Amazon web services (AWS), to host the internal systems and systems in active development, therefore backup is included as a cloud service, and here are some notes on RDS (relational database service) backup strategy:

● When something that may have an effect on Production RDS occurs, a production environment RDS snapshot is created. RDS snapshot creation is automated - e.g. as a pre-step of back-end component deployment with the help of AWS CLI (command line interface).

● Sometimes, it is necessary to create a snapshot at some specific time - in these cases the snapshot is created manually via the AWS console.

● RDS snapshot naming is based on the short name of application, date and time when snapshot creation occurred, e.g. "my-app-cluster-20231006-193214".

● When there is a need to rollback an application's RDS - another RDS is created based on the snapshot. Right after the new RDS from snapshot is ready - the application RDS address is switched.

● Automated snapshots are created for production RDS, and manual for production and non-production RDS.

The company uses Google Workspace, which ensures information integrity and availability is included as a cloud service.

Individual backup procedures must be ensured by a user, if his/her own individual hardware or software solutions are used, but that must be informed and agreed with management. As for individual client projects, different backup procedures and policies may be used and organized from the client side.

Backup and recovery testing

AWS Backup and recovery testing is done manually when ITSS receives a problem request or when an issue is detected. Request or issue is analyzed to assess severity and if the problem relies on a single or multiple hosts and if the problem can be remedied without backup restore. In the latter case

another backup should be created for safety before attempting to recover without backup restore. Proactive, recurring backup and recovery testing is not implemented, as AWS is a cloud environment and provides a layer of security against physical data damage. Backup and recovery testing events are recorded in this log -refer to: "**Backups: history of restore procedures**", available to the administration team.

Configuration management

Configuration management is the process of monitoring the hardware and software configuration of computers and changing configurations when necessary to ensure they stay in line with IT policies. As Exponam allows work from home, this becomes more important as ITSS department no longer has ready access to all computers, which employees are using. Those computers, which may include mobile devices employees bought and set up themselves, may have fallen behind on software patches. Or they might be missing updates to antivirus software. Falling behind on security software updates increases a computer's vulnerability to malware and other forms of attack. Benefits of configuration management: ● Improved user experiences and productivity

● Reduced security vulnerabilities

● Faster time to repair

● Improved IT decision-making

Best practices to ensure successful configuration management:

● Plan, which covers people, processes and technology

Effective configuration management involves people, processes, and technology. It requires planning about how configuration updates will be rolled out, who will manage those updates, how those people will be trained and so on. It also requires well-defined processes for monitoring endpoints and updating endpoints when they are found to be out of compliance with configuration policies. And it requires a process for rapidly deploying patches or making other types of changes to respond to security threats or serious performance problems from recent changes. Plans should be documented and understood by all the relevant stakeholders in the IT department. And those plans should include requirements for configuration tools and for training IT engineers on the use of those tools.

● Being able to monitor on a local network, in a remote location or cloud:

IT organizations need a comprehensive way of managing configurations regardless of where an endpoint is being used. Whether an employee is working in the office, at home, or in some other remote location, the IT organization should be able to monitor and configure that employee's endpoint flawlessly.

● No unmanaged endpoints

To avoid security risks and optimize endpoint performance for employees, IT teams need to put together tools and processes for ensuring that all endpoints regardless of the operating system used have been found and that all changes to those endpoints have been implemented.

● Whenever possible monitor and configure remote endpoints without requiring VPN to access.

That way, no matter where employees are working, the IT team can stay on top of keeping their computers up-to-date and working well. And you'll avoid the problem of employees complaining about the slow network performance that's common with VPNs.

● Avoiding network traffic jams

Use tools for remote access and configuration which does not require a lot of dedicated servers and makes less traffic congestion. Make use of distributed network solutions if possible.

● Result monitoring, problem remediation and continuous improvement.

IT teams should continuously monitor the configurations of endpoints and make changes whenever necessary. To keep track of that ongoing work, it's a good idea to build reporting and trend analysis into your documented configuration management processes. IT and business leaders should be able to receive and see "the big picture" about the state of the computers that employees depend on.

ITSS tries to use these best practices to improve Exponam configuration management.

Network management

Network management best practices ensure that the network is accessible when needed, safe from attackers, scalable to changes of endpoint count:

● Understand the network

Network managers need to have a clear understanding of its structure and components. Importantly it is needed to assess the big picture by mapping out the network topology. Then, identify the type of network (Ethernet, WAN, LAN, etc.) and become familiar with the devices that are used to build it (switches, routers, gateways, etc.). Finally, familiarize yourself with the OSI model, which provides a framework for understanding how data flows through a network. With this information in hand, network managers will be in a much better position to develop a management plan that meets the business's specific needs.

● Identify critical infrastructure and systems

One of the best practices in network management is to identify critical elements and give them priority attention. This means ensuring they are properly configured, monitored, and maintained.

● Implement security best practices

Network security includes policies, processes, and practices for monitoring the network's health, detecting vulnerabilities, and preventing unauthorized access. Understanding network defenses can allow network managers to detect and prevent potential threats more effectively. By regularly

reviewing these elements, administrators can ensure that the network is secure and running efficiently.

● Understanding compliance requirements

Network management is a complex task, and it can be difficult to keep track of all of the different regulations that apply to a business. However, by taking the time to understand compliance requirements, network managers can develop policies and procedures that will keep the network in compliance with laws such as HIPAA, Sarbanes-Oxley, PCI DSS, GDPR.

● Staff training

Employees need to be regularly reminded of basic information security measures, such as password protection and avoiding phishing scams. They also need to be familiar with common network problems and how to resolve them. By ensuring staff are up to date on all aspects of network management, administrators can help to prevent costly disruptions and ensure the network runs like clockwork.

● Monitoring

Monitoring is essential to keeping the network running smoothly. Network managers can quickly establish a baseline for normal behavior and identify potential problems by tracking data from multiple users and devices. In addition, monitoring helps to ensure the high availability of critical systems and eliminates the need for multiple point solutions.

● Disaster recovery

Network administrators must be ready for disasters and plan accordingly, which includes potential hazard identification and strategies for mitigating their effects This may involve data backups, redundant systems, alternate connectivity options and others.

● Task automation

Automating repetitive tasks frees up time for more creative work, leading to a more efficient and effective network management team. For example, network staff may use automated device locators to discover where a device connects to the network, and check application connectivity. Automation can also help verify that each network infrastructure device is linked properly with its neighbor and detect inconsistencies between parts of network configurations and company configuration templates.

● Network testing

Testing is an essential part of network management. By regularly testing the performance of the network, network managers can identify and resolve potential problems before they become disruptive. In addition, testing helps to ensure the network meets the changing needs of the business.

● Gather data for future requirements

Network data can be used to predict future network needs. This is especially valuable when planning for growth or expansion. By understanding how the network is currently being used, network managers can make informed decisions about capacity planning and avoid over or under-buying resources. Network data can also be used to identify trends and spot potential problems. For example, if there is a sudden spike in network traffic, it may be an indication of a distributed denial-of-service (DDoS) attack.

Exponam tries to use these best practices to ensure a safe and reliable network and its management. Exponam uses network segmentation at the office - wired and wireless networks are separated to increase safety and accessibility. Employees use VPN to access critical systems. Network is configured based on UniFi software with an overview of network topology.

7. Documents and records control management

The Information Security Management System (ISMS) of Exponam is a comprehensive framework designed to ensure the protection of information in all its forms. This includes information in written, spoken, electronically recorded, or printed formats. The primary objective of the ISMS is to safeguard information from accidental or intentional unauthorized modification, destruction, or disclosure throughout its entire life cycle.

● Documentation and Accessibility

Within the ISMS, all policies and procedures are meticulously documented. These documents are made readily available to individuals who bear responsibility for their implementation and compliance. This ensures that everyone within the organization is well-informed and equipped to uphold the established standards.

● Recording of Activities

Additionally, all activities identified by the policies and procedures are diligently documented. This practice not only serves as a means of transparency but also aids in traceability and accountability in case of any security incidents or breaches.

● Retention Period

All documentation, regardless of its form, including electronic records, must be retained for a minimum of six (6) years from the time of initial creation. For policies and procedures, this retention period extends to cover any subsequent changes made. This extended retention policy ensures that a historical record of information security practices is maintained.

● Periodic Review

To maintain relevance and effectiveness, all documentation must undergo periodic reviews. The frequency of these reviews will be determined by each entity within Exponam, allowing for flexibility in adapting to specific operational needs and evolving security landscapes.

8. Training and awareness documentation

Any document, policy, rule, or guide may be offered to employees, using e-mail, brown-bag sessions (example presentations, training) or BambooHR system - to receive feedback that employees have reviewed required documentation, the BambooHR system is used to gather a signature from an employee which is kept as a record.

Training and personal development policy

Exponam is committed to the continuous training and development of its employees, both in job related skills training and lifelong learning for personal development. Exponam's employees are one of our greatest assets and helping them develop professionally and personally is crucial to the achievement of the organization's goals. All training practices and procedures will endeavor to support individuals in achieving these goals.

Training and Personal Development Policy has been described in this external document - refer to: "**P100 Training and Personal Development Policy".**

Security training policy

All new users must attend an approved Security Awareness training prior to, or at least within 30 days of, being granted access to any Exponam information resources.

All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect Exponam information resources.

ISO must prepare, maintain, and distribute one or more information security manuals that concisely describe Exponam information security policies and procedures.

ISO must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

9. Internal audit and review

Internal audit:

Exponam conducts annual internal audits to assess the effectiveness of its Information Security Management System (ISMS). The audit program is meticulously planned, considering the status and significance of the processes and areas slated for examination, along with insights gleaned from prior audits.

The audit criteria, scope, frequency, and methodologies should be clearly defined. This selection process for auditors and the conduct of audits are structured to guarantee objectivity and impartiality throughout. Auditors are prohibited from assessing their own work.

The management overseeing the audited area is responsible for swiftly implementing any necessary corrections and corrective actions to rectify identified nonconformities and their underlying causes. Subsequent activities encompass the verification of these corrective measures, with results duly reported.

Comprehensive records of the audits and their outcomes are diligently maintained in accordance with ISO/IEC 27001:2022.

Management review:

Exponam carries out an annual management review once a year to evaluate how effective its Information Security Management System (ISMS) is.

The management review involves a comprehensive assessment that covers the following areas: Progress on Previous Actions: Checking on the advancement of tasks set during prior management reviews to ensure they've been completed and have achieved their intended outcomes. Adaptations in External and Internal Factors: Examining any shifts in circumstances both inside and outside the organization that might affect the Information Security Management System (ISMS). This includes alterations in laws, market conditions, and the organization's structure.

Alterations in Stakeholder Needs and Expectations: Evaluating how the requirements and anticipations of stakeholders and interested parties have evolved. This encompasses clients, regulatory bodies, employees, and other relevant groups. The objective is to guarantee that the ISMS continues to align with these evolving demands.

Feedback assessment: Scrutinizing input received from various sources:

● Identifying noncompliance and taking corrective measures:

Investigating instances of nonconformity and evaluating the effectiveness of the corrective actions taken.

● Evaluating monitoring and measurement outcomes:

Analyzing results from ongoing monitoring and measurement activities to verify the effectiveness of controls and processes.

● Reviewing audit findings:

Going through the outcomes of internal and external audits to identify any areas that require corrective action or improvement.

● Checking goal attainment:

Reviewing the progress made towards achieving established objectives to ensure they are being met as intended.

● Feedback from stakeholders:

Considering input from stakeholders and interested parties regarding how well the ISMS is performing. This information offers valuable insights into areas for improvement and potential enhancements.

● Outcomes of risk assessment and progress of risk treatment plan:

Reviewing the results of the risk assessment process, which includes identifying, evaluating, and addressing risks. Additionally, evaluating the status of the risk treatment plan to ensure that identified risks are being properly managed.

● Identifying opportunities for ongoing enhancement:

Exploring possibilities for improving the effectiveness and efficiency of the ISMS. This might involve initiatives to streamline processes, introduce new technologies, or implement best practices.

This comprehensive review process guarantees that the ISMS remains aligned with the organization's strategic objectives, complies with pertinent requirements, and effectively manages information security risks.

10. Incident recording, monitoring, and mitigation

This section describes the process of managing recording, monitoring, and mitigation of security incidents.

Company uses the Atlassian Jira system and IT service management specifically, to record, monitor and handle incident monitoring and response. Company already uses other Atlassian systems like Confluence and Bitbucket, therefore it offered a simple learning curve and did not require additional funding and time to set up a dedicated server just for incident management. Jira offers incident registering and handling procedures as well as various reports of incident status (open, closed, incidents in mitigation process, incident mitigation time etc.). Incidents are registered manually by ITSS system administrators, security specialists or their managers. There is a plan in consideration to widen incident recording functionality and attach a separate or merge an existing IT support e-mail (support@Exponam.com) to the incident recording system, so that everyone in the company directly could inform about incidents they have met, sending an email. That would also help the incident management team to register delegated information security incident related tasks more easily, using e-mail. However, that would allow reporting also any other IT related issue this way, therefore it is yet in process to develop a robust system on how to structure and manage all received issues and separate them accordingly.

Description of the incident management workflow using Jira:

The IT service management template associates certain requests with an incident management workflow. An incident management workflow helps service project agents to investigate, record, and resolve IT service interruptions or outages and also security related issues with the aim to reduce downtime and negative impacts on business.

Jira Service Management provides an Information Technology Infrastructure Library (ITIL) compliant incident management workflow called ISD: Incident Management workflow for Jira Service Management.

Incident management includes the following high-level process:

● Service end users, monitoring systems, or internal IT members report interruptions. ● The service project agent logs the incident in the service project linking together all reports related to the service interruption.

● The service project automatically records the date and time, reporter name, and a unique ID for the incident.

● A service project agent labels the incidents with appropriate categorization. The team uses these categories during post-incident reviews and for reporting.

● A service project agent prioritizes the incident based on impact and urgency.

● The team diagnoses the incident, the services affected, and possible solutions. Agents communicate with incident reporters to help complete this diagnosis.

● If needed, the service project team escalates the incident to second-line support representatives. These are the people who work regularly on the affected systems.

● The service project team resolves the service interruption and verifies that the fix is successful. The resolution is fully documented for future reference.

● The service project automatically closes the incident.

11. Continual improvement

At Exponam, the commitment to excellence is embedded in our organizational DNA. We are dedicated to the ongoing enhancement of the suitability, adequacy, and effectiveness of our Information Security Management System (ISMS). This process is fundamental in adapting to emerging threats, technological advancements, and evolving business landscapes.

Integral to our continual improvement efforts are the rigorous processes related to monitoring, measurement, analysis, and evaluation of the ISMS. This involves the systematic collection of data and the application of analytical techniques to gain insights into the performance of our information security practices. By examining key performance indicators, we can identify areas for enhancement and take proactive measures to bolster our security posture.

Recognizing the significance of change management and control, our company management has prioritized this aspect. We acknowledge the potential risks associated with ineffective change management and control and, in response, have formulated a comprehensive Change Management and Control Policy. This policy outlines the procedures and protocols to be followed when

implementing changes within our information security framework. It ensures that changes are assessed, authorized, and implemented in a manner that safeguards the integrity of our ISMS.

For detailed guidance on our change management and control Policy - refer to: "**P020 change management and control policy**". This document provides a thorough overview of the policy, including specific procedures and responsibilities involved in managing changes within our information security framework.

In addition to change management, we recognize the critical importance of Business Continuity Management. This encompasses a comprehensive approach to preparing for and mitigating the impact of unforeseen disruptions. Our business continuity and disaster recovery plan are outlined in an external document - refer to: "**P011 Business continuity and disaster recovery plan**". It serves as a blueprint for ensuring the resilience of our operations in the face of adverse events.

Nonconformity and corrective action.

This process of addressing nonconformities and implementing corrective actions is integral to the continual improvement of the ISMS in line with ISO/IEC 27001:2022 standards.

A nonconformity arises when there is a deviation from the established requirements of the Information Security Management System (ISMS) within Exponam. When such a situation occurs, it is imperative to react promptly. This involves acknowledging the nonconformity, documenting the specifics, and initiating a response strategy.

The response strategy may encompass immediate measures to contain and mitigate the impact of the nonconformity. For instance, if a breach is identified, steps will be taken to halt any further unauthorized access and assess the extent of the incident. Simultaneously, consequences will be assessed, which may include notifying relevant parties, initiating legal procedures, or implementing compensatory measures.

After the initial reaction, a comprehensive evaluation of the nonconformity is conducted. This involves a multifaceted approach:

Reviewing: Thoroughly examining the circumstances surrounding the nonconformity. This includes scrutinizing relevant documentation, interviews, and any available electronic records. Determining the Causes: Identifying the root causes that led to the nonconformity. This involves a systematic analysis to pinpoint the underlying factors contributing to the deviation.

Assessing Similarities and Potential Recurrence: An assessment is made to determine if similar nonconformities have occurred in the past or if there is a likelihood of similar incidents happening in the future. This foresight is essential for proactively preventing future occurrences.

Based on the evaluation, a corrective action plan is devised. This plan outlines specific steps to rectify the nonconformity and prevent its recurrence. This could involve revising processes, enhancing controls, providing additional training, or implementing technological safeguards.

Once the corrective actions are implemented, their effectiveness is rigorously reviewed. This entails a careful examination to ensure that the corrective measures have effectively addressed the nonconformity and that there are no unintended consequences.

If necessary, adjustments to policies, procedures, or controls may be made based on the lessons learned from nonconformity.

The incident recording, monitoring, and mitigation process is described separately according to this external policy - refer to: "**P018 Information Security Incident Management Policy**".

12. Documented information on ISMS performance

The organization has determined the following points that need to be monitored and measured, including information security processes and controls:

- Context of the Organization
- Leadership and Commitment
- Planning
- Support
- Operation
- Performance Evaluation (This process involves evaluating the performance of the ISMS and determining if it aligns with the organization's objectives and requirements):
  - Monitoring, Measurement, Analysis, and Evaluation: Review the processes for monitoring and measuring information security performance.
  - Internal Audit
  - Management Review
- Improvement
- Documentation and Records
- Compliance
- Third-Party Relationships
- Business Continuity and Disaster Recovery
- Cybersecurity

The evaluation process should be systematic, and findings should be thoroughly documented.

13. Legal and regulatory compliance

Documents related to compliance with legal and regulatory requirements, including privacy laws and industry-specific standards.

The information security policy applies to all users of Exponam information including employees, students, volunteers, and outside affiliates. Failure to comply with Information Security Policies and Standards by employees, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Exponam procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with Information Security Policies and Standards by students may constitute grounds for corrective action in accordance with Exponam procedures. Further, penalties associated with state and federal laws may apply.

Possible disciplinary/corrective action may be instituted for, but is not limited to the following: ● Unauthorized disclosure of a sign-on code (user id) or password.

● Attempting to obtain a sign-on code or password that belongs to another person. ● Using or attempting to use another person's sign-on code or password.

● Installing or using unlicensed software on Exponam computers.

● The intentional unauthorized destruction of Exponam information.

● Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

● Discovering internal and external non-public projects information.

At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such an entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

The purpose of this policy is to provide high-level guidance regarding key aspects of human resource management, including work health and safety, anti-discrimination and harassment measures, attendance and absence rules, work performance management and evaluation approach, as well as overall key roles in the Company and their contact information.

Human resources policy has been described in this external document - refer to: “**P050 Human Resources Policy”.**

These are active human resource guidelines and rules described in these external documents: ● **Communication guidelines** - refer to: “**Communication guidelines_v1.0**”.

● **Time - off policies and instructions** - refer to: "**Time-Off_Policies_Instructions_082020**". ● **Internal working rules** - refer to: "**Internal working rules_v1.0_ENG_LV_2020**". ● **Kitchen usage guidelines** - refer to: "**Kitchen usage guidelines**".

Personal data protection policy

The Personal Data Protection Policy outlines the company's commitment to protecting personal information that it collects, processes, and stores. The policy specifies the responsibilities of employees and contractors, and provides guidance on the appropriate use, retention, and destruction of personal data. It also addresses the rights of data subjects, including access, correction, and erasure, and establishes procedures for responding to data breaches. The policy emphasizes compliance with relevant laws and regulations related to data protection and privacy, and the importance of maintaining trust and confidence with stakeholders regarding the company's handling of personal data.

Personal Data Protection Policy has been described in this external document - refer to: "**Personal data protection policy".**

Anti-bribery and anti-corruption policy

The Company is committed to upholding all laws relevant to countering bribery and corruption in each of the jurisdictions in which it operates, conducting all its business in an honest and ethical manner. Exponam takes a zero-tolerance approach to bribery and corruption in any form (including, but not limited to direct and indirect bribes, inducements, kickbacks, extortion) and is committed to acting fairly and with professional integrity in all its business dealings and relationships. It is the goal of Exponam to avoid acts which might reflect adversely upon its integrity and reputation.

Anti-Bribery and Anti-Corruption Policy has been described in this external document - refer to: "**P021 Anti-Bribery and Anti-Corruption Policy".**

Background check policy

The purpose of this policy and performing background checks is to determine and or confirm the qualifications and suitability of a job candidate for the position for which the candidate is being considered, and to help ensure the safety of our work environment. The Company reserves the right to perform background checks in any situation when it is deemed appropriate to protect the interests of the Company or address client requests.

Background check Policy has been described in this external document - refer to: "**P055 Background check Policy"**.

Code of conduct

The purpose of this corporate Code of Conduct (the "Code") is to articulate the fundamental ethical and professional standards and principles that are to guide the employees as well as to all individuals who perform services for Exponam pursuant to a consulting agreement or similar arrangement (including full and part-time employees, temporary employees, independent contractors, consultants,

advisors and third-party service providers). Accordingly, all references herein to “employees” shall apply to all employees and individuals who perform such or similar services described in the foregoing sentence.

The Code includes affirmations of policies contained in greater detail in Exponam’s policy manuals and procedures. All references herein to any policies, procedures, and standards shall apply to such policies and procedures as the same may be amended from time to time and/or replaced by applicable Exponam-wide policies, procedures, and standards.

Code Of Conduct has been described in this external document - refer to: “**P110 Code of conduct”.**

13. Supplier and third-party management

Procedures for assessing, selecting, and managing third-party vendors with access to sensitive information.

This policy outlines responsible sourcing of products and services from its suppliers, including subcontractors. In today’s global market, products and services are typically sourced from a variety of locations nationally and internationally, thus emphasizing the importance of adhering to clear guidelines, to ensure that:

● Exponam is sourcing all products and services in a responsible, ethical manner;

● Exponam works towards improving its social and environmental practices;

● Exponam commits to working with suppliers that maintain the same high standards; ● Exponam corporate and brand reputation is adequately protected.

Responsible Sourcing Policy has been described in this external document - refer to: “**P022 Responsible Sourcing Policy”.**

Exponam carefully investigates terms of services whenever using third party services (AWS, Google Workspace, Azure), so that they are following all necessary legal and regulatory requirements.

14. Communication and reporting

The following core principles will guide information security matters processing activities:

● All employees and contractors of the Company shall be made aware of the procedure for reporting information security matters and their responsibility to report such.

● All information security matters shall be reported promptly to the helpdesk (**support@exponam.com**).

● The severity of the information security matters shall be assessed, and the Company management response shall be proportionate to the threat.

● Key information about serious information security matters (i.e., those of severity *High* or *Very high*), including the impact of the incident (financial or otherwise), shall be formally recorded and the records shall be analyzed to assess the effectiveness of information security controls.

● New risks identified because of an incident shall be assigned to the relevant risk owner and processed further in accordance with the Company's "**P030 Corporate Risk Management Policy**".

● Incidents should be reported through the chain of command (employee to manager), so the incident may be properly recorded and analyzed and shall be further reported to higher management or the appropriate external authorities where relevant.

● Management should decide whether the external parties need to be informed about information security matters.