Information Security

A DESCRIPTION OF INFORMATION SECURITY WORK AT LOGIQ AS

Contents

Logiq Information Security Policy

Policy

The Board of Directors and management of ***Logiq AS*** located at ***Halden, Norway,*** operates primarily in the business of ***IT-services for digital trade.***

We are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information and information-related assets to meet the purpose and goals of the organization.

Information and information security requirements will continue to be aligned with the organization's business goals and will consider the internal and external issues affecting the organization and the requirements of interested parties.

Our ISMS (Information Security Management System) objectives are outlined and measured in accordance with the requirements of the ISO/IEC 27001.

The ISMS is intended as a mechanism for managing information security related risks and improving the organization to help deliver its overall purpose and goals.

Our risk management approach provides the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of our ISMS.

The approach taken towards Risk Assessment and management, the Statement of Applicability and the wider requirements set out for meeting ISO 27001 identify how information security and related risks are addressed.

The Management Board is responsible for the overall management and maintenance of the risk treatment plan with specific risk management activity tasked to the appropriate owner within the organization. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks, for example during special projects that are completed within the context.

Control objectives for each of these areas are supported by specific documented policies and procedures in the online environment and they align with the comprehensive controls listed in Annex A of the ISO 27001 standard.

All employees and relevant Interested Parties associated to the ISMS have to comply with this policy. Appropriate training and materials to support it are available for those in scope of the ISMS and communication forums such as the ISMS communications group are available to ensure engagement on an ongoing basis.

The ISMS is subject to review and improvement by the Management Board which is chaired by CISO and has ongoing senior representation from appropriate parts of the organization. Other executives/specialists needed to support the ISMS framework and to periodically review the security policy and broader ISMS are invited in the Board meetings and complete relevant work as required, all of which is documented in accordance with the standard.

We are committed to achieving and maintaining certification of the ISMS to ISO 27001 along with other relevant accreditations against which our organization has sought certification.

This policy will be reviewed regularly to respond to any changes in the business, its risk assessment or risk treatment plan, and at least annually.

Definitions

In this policy and the related set of policies contained within the online environment that incorporate our ISMS "information security" is defined as:

preserving

This means that all relevant Interested Parties have, and will be made aware of, their responsibilities that are defined in their job descriptions or contracts to act in accordance with the requirements of the ISMS. The consequences of not doing so are described in the Code of Conduct. All relevant Interested Parties will receive information security awareness training and more specialized resources will receive appropriately specialized information security training.

the availability

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The environment must be resilient, and the organization must be able to detect and respond rapidly to incidents or events that threaten the continued availability of assets, systems and information.

confidentiality

This involves ensuring that information is only accessible to those authorized to access it and preventing both deliberate and accidental unauthorized access to the organizations and relevant Interested Parties information, proprietary knowledge, assets, and other systems in scope.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification, of either physical assets or electronic data.

of information and other relevant assets

The information can include digital information, printed or written on paper, transmitted by any means, or spoken in conversation, as well as information stored electronically. Assets include all information-based processing devices owned by the organization or those of relevant Interested Parties and BYOD in scope that are processing organization related information.

of our organization

The organization and relevant Interested Parties that are within the scope of the ISMS have signed up to our security policy and accepted our ISMS.

Information Security Management

Scope

The scope of Logiq's ISMS has been defined as follows:
"Protection of data in the design, development, operation, maintenance, technical support, sales, and marketing of Logiq and for customers and partners worldwide."

Information Security Management System (ISMS)

In 2019/2020 Logiq introduced a dedicated Information Security Management System (ISMS), based on ISO 27001 standard to strengthen and maintain continuous, structured, and controlled work with information security. The system ensures that Logiq follows its own goals and objectives to prevent, detect and manage information security challenges.

More detailed descriptions from Logiq's information security policies may be presented to Logiq customers or relevant stakeholders upon justified request.

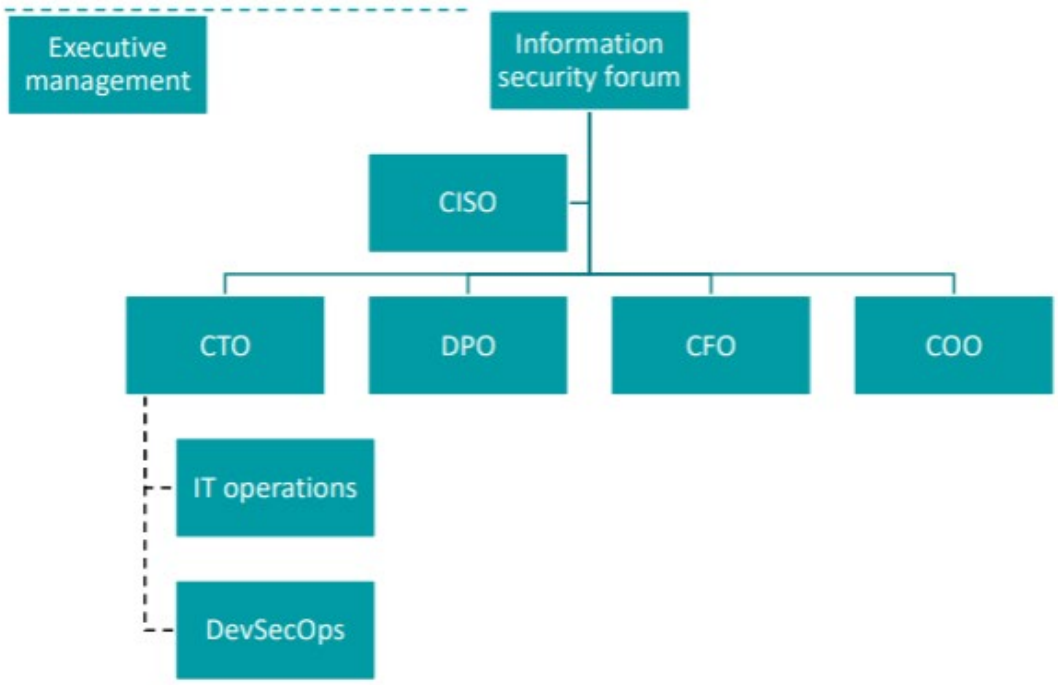

Figure 1 – Information Security Organization Chart

Risk Assessment and Treatment Methodology

The effective management of information security has always been a priority for Logiq to manage risk and safeguard its reputation in the marketplace. However, there is still much to be gained by Logiq in continuing to introduce industry-standard good practice processes.

Logiq has adopted ISO/IEC 27001 as an effective way to put in place an information security management system (ISMS) to ensure that our objectives remain current and our processes, policies and controls are continually improved.

It is important that Logiq has an effective risk assessment and treatment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them. In addition, the process should be sufficiently clear so that successive assessments produce consistent, valid and comparable results, even when carried out by different people. We have adopted ISO/IEC 27005 as the foundational framework for our risk management practices.

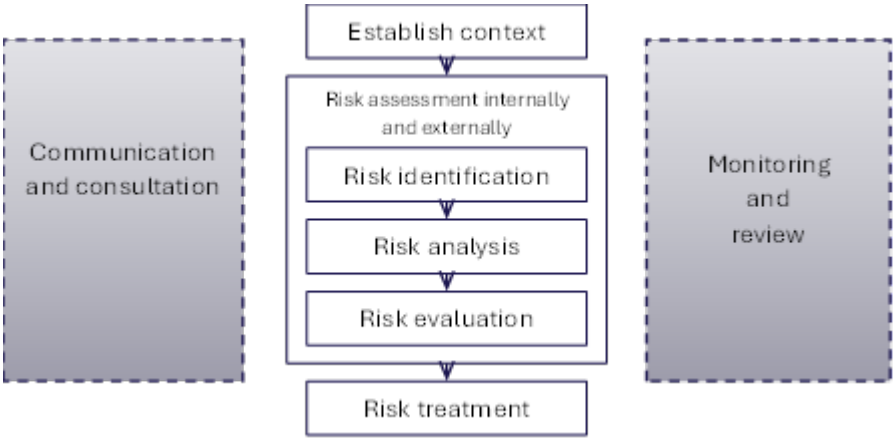

Figure 2 Risk management summary

Information Classification and Handling

We ensure identification and understanding of protection needs of information in accordance with its importance to the organization and especially to protect privacy and personally identifiable information (PII).

We recognize the importance of effective information classification appropriate handling to protect information and associated assets based on their value and importance.

Our classification policy is based on:

- Extensive risk assessment
- Requirements for the confidentiality, integrity; and availability of information and associated assets
- Pragmatic rules to balance security requirements against efficacy of working practices

Access Management

We ensure secure and appropriate access to systems and data through a comprehensive access management approach. Our access management is based on the key principles of:

- Deny-by-default
- Need-to-know

- Least privilege
- Privacy by default
- Role-based access control (RBAC)

We manage access rights through clearly defined roles and responsibilities, ensuring users are granted access strictly based on business need. Our access control mechanisms use a combination of role-based access, least privilege principles, and continuous monitoring. Identity management verifies and manages user identities across the organization. We also enforce strong authentication measures including multi-factor authentication to validate user access and prevent unauthorized entry.

Physical and Environmental Security

Logiq understands the importance of physical security and environmental security in protecting the security of information assets and the privacy of Personally Identifiable Information (PII). All our office locations and physical assets are secured using well-defined physical access controls ensuring that only authorized personnel can enter our premises.

Operational and Technical Security

Incident Management

We ensure quick effective, consistent and orderly response to security and privacy incidents, including communication on information security and privacy events.

Log and Event Monitoring

We implement comprehensive logging and event monitoring to support our information security objectives. We record events, generate evidence, ensure the integrity of log information, prevent unauthorized access, identify information security and privacy events that can lead to an information security or privacy incident, supporting timely response and effective investigations.

Secure System Development

We embed information security and privacy into every phase of our development lifecycle. We consider information security at each step from design to deployment, to ensure that our software and systems are built with security in mind. Our system development subject to the principles of defensive coding, privacy by design, privacy by default and minimization of PII processing.

Change Management

We preserve information security, privacy, and the protection of personally identifiable information (PII) when executing changes to the organization’s information systems, software, infrastructure, and third-party integrations.

Our change management policy ensures that all changes are correctly assessed and managed and include adequate and proportionate consideration in relation to information security and privacy aspects. Changes to the organization, business processes, information processing facilities, and

systems that effect information security and privacy are adequately controlled via our change management process.

Business Continuity and Disaster Recovery

We are committed to maintaining operational resilience through well-defined business continuity and disaster recovery plans. Our strategies are designed to minimize disruption, protect critical services, and ensure rapid recovery in the event of security incidents. Regular testing, backup procedures, redundancy, and risk assessments help us stay prepared and responsive, ensuring continuity of service securely for our customers and partners.

Cybersecurity Awareness Program

Information security awareness, education and training are delivered to staff and, where necessary, contractors and other interested parties as part of their onboarding to the organization. We utilize a learning platform for comprehensive training and awareness purposes. Our key activities include tailored information security courses, regular phishing campaigns, and regular awareness materials for the staffs.

Communication and Contact

If you have any question about our information security program or wish to report a potential vulnerability, please contact us at itsecurity@logiq.no.