Security- and resilience-policy

Information

Gjensidige

Purpose

The purpose of this Group Policy is to define information security and resilience principles as part of the Gjensidige Information and communication technology (ICT) risk management framework to protect Gjensidige's information values and ensure information security risk management of high standard and compliance with applicable regulations.

Scope / target

This Policy applies to Gjensidige Forsikring ASA with subsidiaries integrated in the group insurance ICT infrastructure or regulated by the financial authority (hereinafter referred to as Gjensidige).

Information Security Policy

This policy shall set the direction and overall guideline for information security activities in Gjensidige within the ICT risk management framework to ensure security and resilience in business operations.

Information security objectives

Gjensidige acknowledges that it is not possible to protect against all sorts of security events or eliminating all risks, however, systematic information security activities and skilled employees shall demonstrate low operational risk within Gjensidige's risk appetite.

A comprehensive ICT risk management framework with an effective Information Security Management System (ISMS), shall support the ability to preserve high availability, authenticity, integrity and confidentiality of information and data processed in Gjensidige. The framework shall also cover security requirements when using third party suppliers.

The governing structure shall be founded on International Organization for Standardization (ISO) standards and leading best practice and efficient and effective Information security controls shall be implemented and utilised using modern security technology.

Organizational security

CEO is responsible for the information security in Gjensidige and shall ensure an effective and adequate security organization.

A second-line information security function, known as Group Security, operates independently from day-to-day security operations and is headed by a Chief Security Officer (CSO). Its role is to assist the CEO in fulfilling this task.

1st line shall implement security requirements put forward by the ISMS as well as continuously monitor the effectiveness of the security controls on the current operating environment, in line with a dynamic threat and risk landscape. The IT-security department will have special responsibility for implementation and monitoring of technical security controls.

People security

Gjensidige seeks an information security culture that is characterized by a high level of individual responsibility and the ability to safeguard and protect the information we process.

Information security should seamlessly integrate as a fundamental and continuous component for all employees and externally hired resources. A continuous information security awareness program shall ensure that employees possess a comprehensive understanding of risk and are equipped with the skills to implement sound information security practices in their daily activities.

Access to – and processing of – information shall follow the principle of "least privilege" and "need to know" according to role and service needs. The same applies to use of IT systems and infrastructure. Privileged access shall be limited, subject to special control, and only granted when necessary to perform tasks.

Physical security

Physical and environmental security shall ensure effective physical protection of Gjensidige's information, assets, personnel, and their surroundings. All offices where Gjensidige operates shall have adequate physical security against unauthorized access and other undesirable incidents.

Life and health should always be the highest priority when we assess, design, and implement physical and environmental security measures.

Technological Security

Security controls in Gjensidige's IT systems and infrastructure shall continuously be adapted to the threat landscape and provide the correct level of protection of Gjensidige's information values and other assets.

Sufficient monitoring of the infrastructure and information systems shall ensure that security incidents and deviations can be detected, handled, and mitigated in a timely and adequate manner.

Potential vulnerabilities in IT-systems and infrastructure shall be identified systematically and mitigated timely when security deviations and vulnerabilities are found.

Classification and risk assessments of information, information systems, business processes and assets shall form the baseline for relevant and adequate security controls throughout the operation. Change of business operation shall at no point be able to reduce existing and approved level of information security.

Business continuity and resilience policy

The ICT risk management framework shall be supported by a Business Continuity Management System (BCMS) to ensure resilience from disruptions. Well trained crises management teams shall prepare for, respond to and, and be able to recover critical business processes disruptions.

Technical preparations and controls shall ensure a resilient ICT infrastructure that able Gjensidige to restore return to normal operation in a timely manner if an crises event or major incident occurs.

Business Impact Assessments (BIA) shall ensure that relevant business processes are identified, prioritized, and linked to relevant IT systems and other assets.