# Information Security Policy

| | |
|---|---|
| Owner | CIO |
| Approved by, date | The Board, 2021-06-23 |
| Version | 1.5 |

## Background

Information is one of the most important strategical resources in Byggfakta Group business. Therefore, it is crucial to protect information at a sufficient level based on:

- Secrecy, information is not made available or revealed to unauthorized person
- Correctness, information is correct, current and complete
- Availability, information is accessible and useful for authorized person
- Traceability, change end events in information processing can be traced

Information security is divided into two areas: administrative security and technical security.

Administrative security includes organization, steering, roles and responsibility like regulations and processes.

Technical security also called IT security or Cyber security includes network, servers, workstations, hardware, software, datacenter, backups etc.

## Goal

Information security for Byggfakta Group has following goals:

- All documents and instructions regarding information security must follow the instructions in Information Security Policy
- All employees in Byggfakta Group companies should have knowledge of the Information Security Policy
- The Information Security work should be performed in a structured and planned way and improve quality, efficiency and strengthen integrity
- Information Security includes:
    - Information classification
    - Threat and risk analysis
    - Incident management
    - Business Continuity Planning
    - Traceability for actions and transactions
    - Follow-up, actions and feedback
    - Education of employees
- There should be a communication plan that can be used in case of incident effecting information security.
- Information should be protected in parity to the value and sensitivity of the information
- There should be documentation on all business-critical IT systems
- Legal requirements on information should be met
- Information Security practice should be updated to meet the new demands of the outside world
- Threat against information should continuous be analyzed to meet the demand in case of a crises

- All critical incidents that affect information security must be reported to IT service desk and immediate supervisor and those incidents should be solved promptly.

## Principle

Information security policy is the base for handling information security. Based on Information security and IT policy there are IT guidelines and instructions (Appendix) that steer the work to meet the overall goal for information security.

Information resource have reference to all information irrespective of it is stored and processed in an IT system, is printed on paper, noted in a notebook, orally communicated. Even movies, pictures and audio recording are included in the definition.

Two key roles in information security are system owner and information owner.

## Responsibility and roles

Byggfakta Group has a decentralized IT organization, where each business unit has it's own IT department. CIO/CTO report status and progress in the IT area to IT Board of the business unit. Members of the BU's IT board are local CEO, CFO and CIO/CTO.

| Role and group | Responsibility and obligation |
|---|---|
| **IT Board** | • Approve the Information Security Policy |
| **BU's CEOs or CFOs** | • Responsible for Information Security Policy and surrounding framework.<br>• Ensure that change in Information Security are preceded by financial and risk-based analysis.<br>• Responsible for segregation of duties routines.<br>• Overall responsible for implement and verify Information Security Policy |
| **BU's CEOs** | • Responsible for the compliance of the policy in their organization |
| **BU's CIOs/CTOs** | • Responsible that the IT environment is compliant to the policy |
| **Information owner** | • Overall responsibility for how information can be managed regardless of what system or media the information is stored in<br>• Ensure information is classified and that information security requirements are met independent of system or media for the information |
| **System owner/Product owner** | • Functionality responsibility for how systems manage information<br>• Conduct the necessary risk-analyzes<br>• Ensure agreement with external parties for information security exist and complied with<br>• Change Management for system meets the requirement in the Policy<br>• Establish and document system access requirement<br>• Backup plan in case of interruption<br>• Regular monitoring of compliance for the Policy and guidelines |

| | |
|---|---|
| **Immediate supervisor** | • Responsible for routines and instruction needed to meet the Information Security Policy |
| **Employee** | • Know and follow the Information Security Policy and other documented routines associated with the employee responsibility<br>• Report incidents, events and deviation that can affect Information Security |

## Organization for information security

Information should be classified based on risk matrix below.

| | **Consequence** | **Secrecy** | **Correctness** | **Availability** |
|---|---|---|---|---|
| **3** | Serious | S3<br>Serious negative impact on own or other organization, or on individual. | C3<br>Serious negative impact on own or other organization, or on individual. | A3<br>Serious negative impact on own or other organization, or on individual. |
| **2** | Significant | S2<br>Significant negative impact on own or other organization, or on individual. | C2<br>Significant negative impact on own or other organization, or on individual. | A2<br>Significant negative impact on own or other organization, or on individual. |
| **1** | Moderate | S1<br>Moderate negative impact on own or other organization, or on individual. | C1<br>Moderate negative impact on own or other organization, or on individual. | A1<br>Moderate negative impact on own or other organization, or on individual. |

## Compliance

To meet the requirements specified in this policy following should be done annually:

- Review created information security incidents and actions to avoid future similar incidents
- Review and update policy and guidelines documents
- Executing IT general controls

## Penalties for infringement

Violation of IT policy can be ground for dismissal.