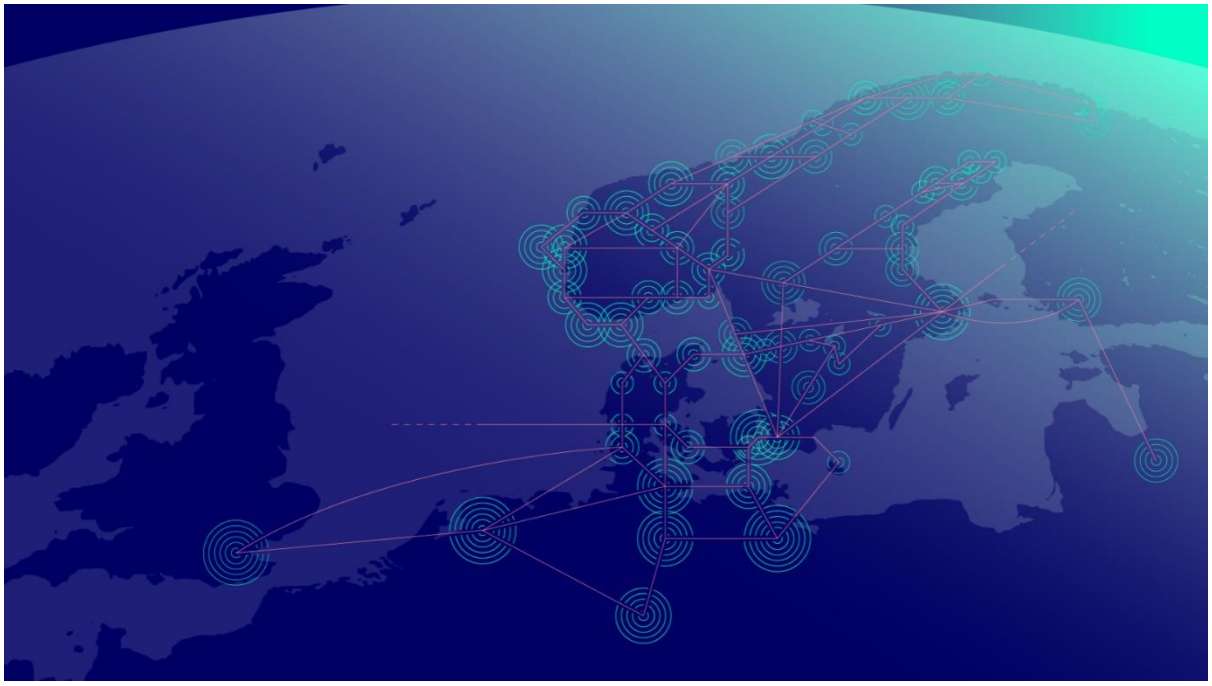
GlobalConnect

- Group Security Statement

Date: 25. Sept. 2020
Approved by: Group Chief Security Officer
Version 1.0

GlobalConnect

Table of contents



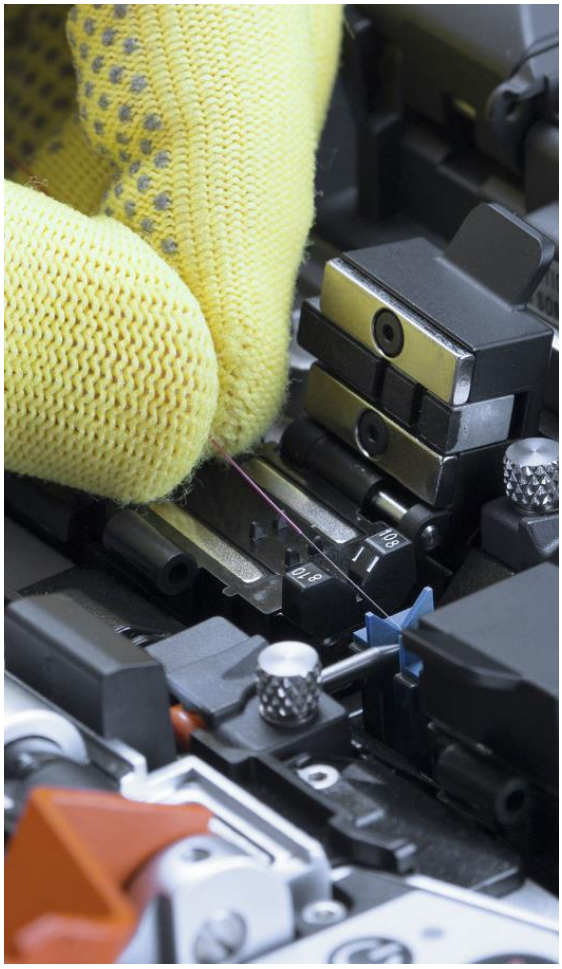
Overview

GlobalConnect works systematically to secure personnel, assets and infrastructure from relevant threats and vulnerabilities. GlobalConnect has a risk-based approach to security where implemented security measures aims to balance risk exposure, business value, vulnerabilities and threats.

This security statement provides an overview of the security controls integrated in GlobalConnect.

Purpose

The purpose of this statement is to inform about GlobalConnect's security work which objective is to establish, and continuously improve, a trustworthy and adequate level of security to support and enable business goals in an efficient manner in compliance with internal, legal and contractual requirements.



Group Policy – Security

GlobalConnect's Board of Directors issues the *Group Policy – Security.* The policy establishes the organization's security principles and requirements. The requirements aim to protect business values by having security measures which protect and preserve assets such as personnel, customers, information, infrastructure, internal and public networks, as well as office buildings and technical facilities. The Group Policy applies to GlobalConnect and its Subsidiaries as a binding policy. It applies to all directors, managers, employees, consultants and contractors working for or on behalf of the company.

GlobalConnect continuously works towards promoting the policy's principles and a culture of security and risk awareness by means of communication and training activities.

Security Governance

GlobalConnect has established a Security Management System which incorporates Cyber and Information Security management, Personnel and Physical security management, Crisis Management and Risk management. The overall Security Governance is coordinated by Group Security and security measures are implemented, operated and maintained in collaboration with the entire organization.

The central security objectives are:

- Securing the organizations assets and shareholders' value.
- Ensure that customers' expectations and business agreements are met.
- Ensure compliancy to applicable laws, regulations, and contractual security related requirements.
- Ensure that the organizations objectives and strategies are not jeopardized due to security weaknesses.

The Security Management System specifies requirements within security and security risk management across all organizational entities and is continuously and methodically evaluated, maintained and improved.

The Security Management System ensures:

- That security risks are addressed and, as required, mitigated.
- Alignment and compliance with internal and external security requirements.
- A continuous focus on maintaining a security and security risk awareness culture.
- That security policy, instructions and directives are aligned with the organizations objectives and strategies.

The Security Management System defines security roles and responsibilities within the organization. The security responsibilities are implemented and managed within the line organization. All parts of GlobalConnect are governed under the Security Management System. Annual security compliance assurance activities are carefully planned, based on and prioritized according to assessed risk, and carried out within all organizational levels and departments.

Security Organization

The Group CEO is accountable for the implementation of the Group Policy - Security. The Group executives reporting to the Group CEO are responsible for ensuring that the policy is communicated and implemented, and that personnel within his/her area of responsibility are familiar with and comply with the Group Policy.

GlobalConnect has a formal Group Security organization led by the Group Chief Security Officer (CSO), who acts on behalf of the Group CEO. The CSO has the overall responsibility for security governance in GlobalConnect, including the responsibility for all governing documents regarding security.

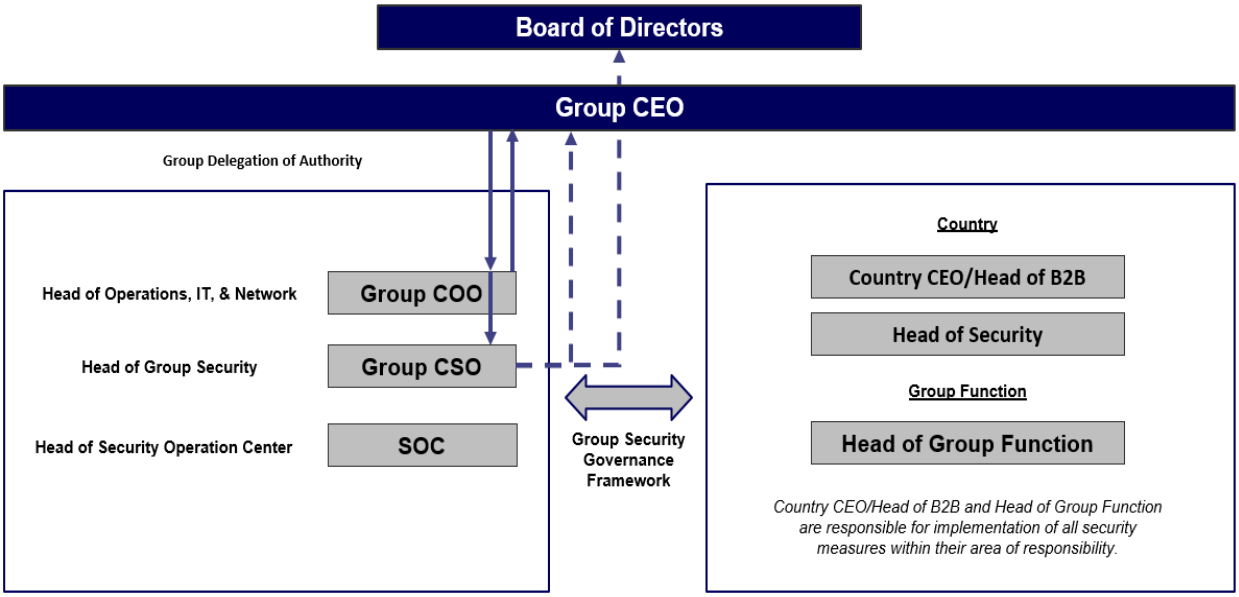
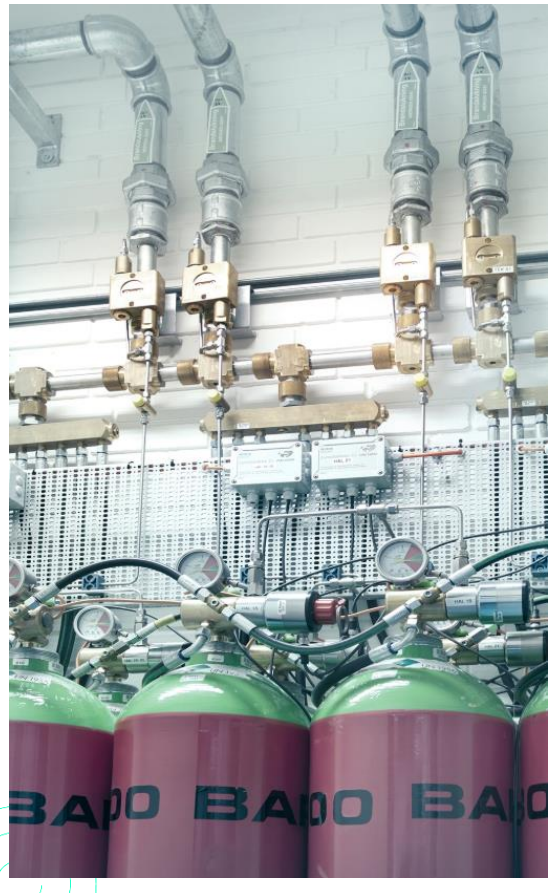


Figure 1:
GlobalConnect's Security organization



Security Risk Management

Risk management is a fundamental part of security management in GlobalConnect, and a prerequisite for effective and efficient security controls and alignment with the company's risk appetite.

The security risk management process is aligned with the company's overall enterprise risk management framework. This framework is based on the ISO 31000 risk management standard and the COSO ERM guidelines, both widely recognized as best practice within the field of risk management. Within the security domain, GlobalConnect also uses the three factor approach (value-threat-vulnerability) to assess risk against intentional undesirable actions.

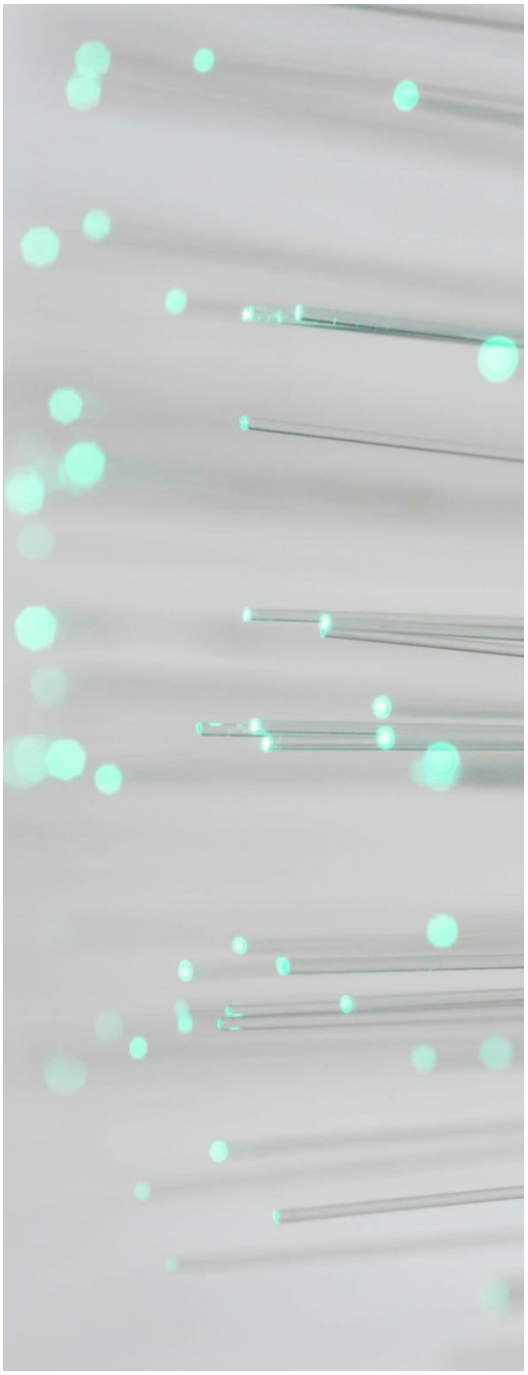
To ensure an effective and targeted information security management system (ISMS), GlobalConnect has also implemented a specific security risk management process based on the ISO 27005 standard. This ensures:

- Systematic identification and prioritization of assets
- Identification and evaluation of relevant threats, vulnerabilities and existing controls
- Thorough analysis and evaluation of identified risks
- Implementation of effective and efficient controls to ensure that our assets operates within acceptable risk levels

Information security

In GlobalConnect information security is defined as preservation of confidentiality, integrity and availability of information.

- *Confidentiality* is the property that information is not made available or disclosed to unauthorized individuals, entities or processes.
- *Integrity* is the property of accuracy and completeness.
- *Availability* is the property of information being accessible and usable upon demand by an authorized entity.



The protection of GlobalConnect's information is crucial during its whole lifecycle. Security measures are implemented in accordance with the information's sensitivity.

Information classification defines the appropriate level of protection. Information in GlobalConnect is classified in order to:

- Identify the sensitivity of information, in terms of the likely impact resulting from unauthorized disclosure, loss or manipulation with regards to its value and/or criticality.
- Enable appropriate handling and protection during its lifecycle, based on business, legal and contractual requirements.

Information classification applies to all information in different formats such as:

- Information in electronic form
- Electronic communications
- Information in physical form
- Spoken information

Personnel Security

GlobalConnect's personnel security consists of several policies and procedures which seeks to mitigate the risk of personnel exploiting their legitimate access to the organization's assets for unauthorized purposes. It also aims to safeguard personnel from outside threats and harm.

Implemented Personnel Security measures in GlobalConnect has the following objectives:

- Reduce the risk of fraud, theft and misuse of assets such as information, facilities and resources.
- Ensure that personnel and contractors are suited for and understand their role and area of responsibility.
- Safeguard personnel from outside threats and harm.

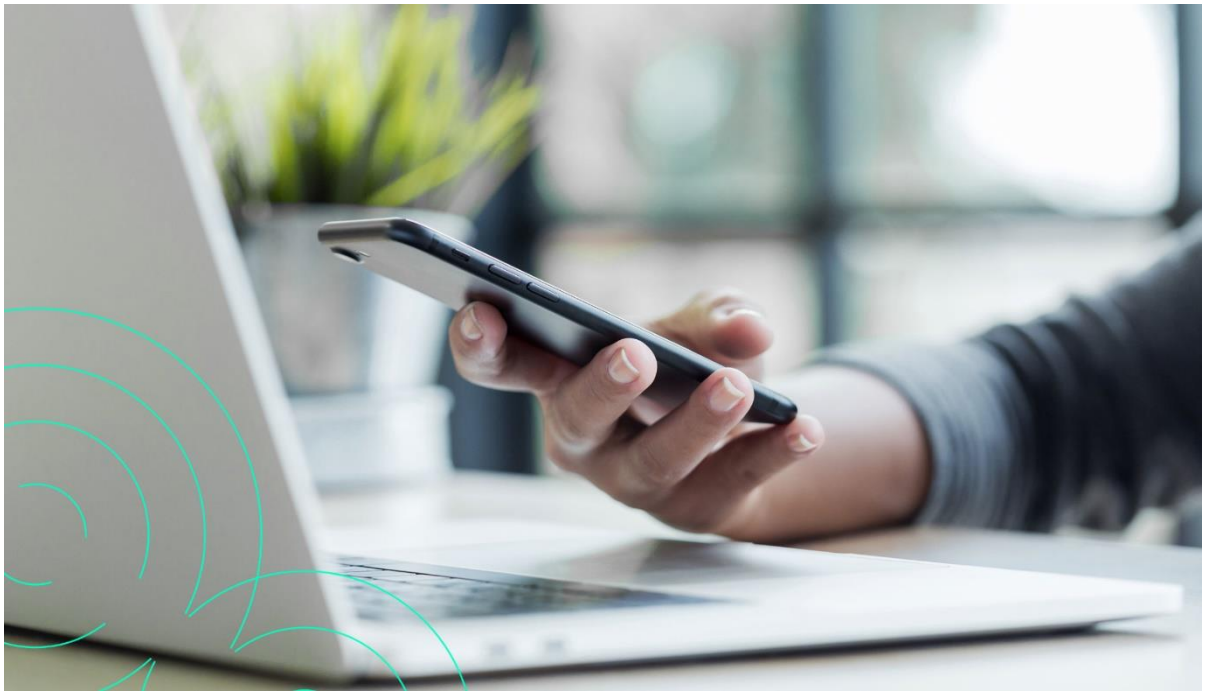
GlobalConnect's Group Security oversee the screening process and handles all security clearances prior to and during employment. All new hires must undergo an onboarding process where role and area of responsibilities are made familiar. All personnel are obliged to sign confidentiality agreements.

GlobalConnect continuously work towards promoting a culture of security and risk awareness amongst its employees by means of communication and training activities during employment.

GlobalConnect has an established and documented offboarding process that defines responsibilities for returning company assets and removal of access rights.

Human resources

Background checks are performed in the recruitment process prior to employment. Personnel intended for key positions undergo detailed screenings and security clearance.



Multiple layers

The essence of Physical security is defense in depth. The deployment of multiple barriers to the most valuable or sensitive areas and information ensures that protection is not dependent on the success or failure of one single barrier. For physical access this means protection by physically dividing areas into different security zones. Barriers in GlobalConnect are both physical and logical.

Visibility and identification

It is mandatory to wear access cards visible while being in, or around, GlobalConnect's offices and infrastructure. In addition to be an electronic key that open doors, the access card serve as a badge identifying the cardholder. The badge information makes it easy to identify each other and to ensure that no one are let into a security zone that exceed their access level.

Monitoring

All usage of, and access to, GlobalConnect's infrastructure is monitored and logged. Audits of access privileges are performed on a regular basis.

Physical Security

Role-based access

GlobalConnect use e.g. role-based access control (RBAC), and access to any of GlobalConnect's infrastructure is stringently based on the subject's role in the organization, and possessed privileges is per the limitation of job responsibilities.

Offices or technical facilities that are regularly visited by customers, and other business contacts have strict routines for handling visits.

All contractor and service personnel must be able to confirm their identity. Entrusted and security cleared contractors will be issued a *GlobalConnect contractor access card*. Others will be issued with direct supervision.

Access Control

GlobalConnect follows a formal process to grant or revoke access to its assets i.e. information, IT systems, physical and logical infrastructure. Access rights are stringently based on the subject's role in the organization, and possessed privileges is per the limitation of defined responsibilities.

The Organization uses a combination of role-based and rule-based access control approaches. GlobalConnect has established documented procedures for secure creation and deletion of user accounts and access, including processes to disable and/or delete accounts and access rights.

The responsibilities for implementing access control in ordinary operations, including managing and reviewing, lies within the line organization.

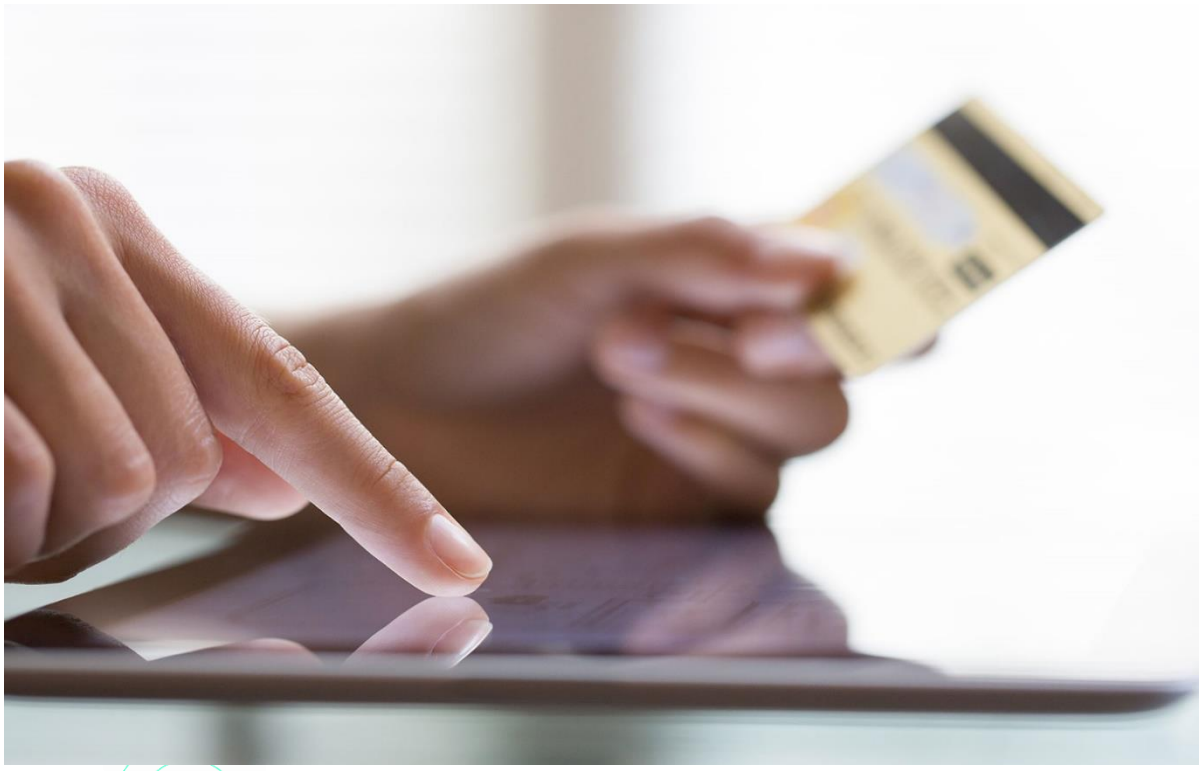
Access control policies

The organizations access control policies establish the requirements for access control e.g. authentication methods like login with user ID and password, regular password changes, password reuse restrictions and minimum password complexity. GlobalConnect requires clear desk and clear screen practices e.g. the use of screensavers that reactivate after a period of inactivity and forces a re-authentication. All personnel are required to take reasonable precautions to protect the confidentiality of security credentials.

Computer security and remote access

All GlobalConnect desktops and laptops are protected by hard drive encryption software. The software enforces password controls and uses a dynamic password time-out to prevent brute force password attacks. Additionally, the software is bound to the hard drive, protecting not only the operating system, but also the data.

GlobalConnect uses virtual private network (VPN) software to enable secure, internet-based remote access for its personnel. VPN users are required to authenticate using multi-factor authentication (MFA).

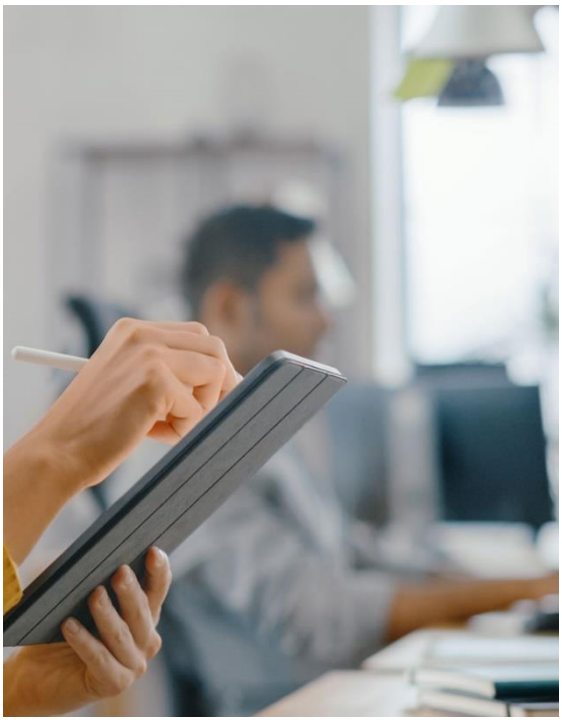


Communications and Operations Management

GlobalConnect has established and maintains control over a repository of procedures, formal review and approval processes, and revision management. During the entire life cycle of products, services, strategic and operational processes, spanning from acquisition, development and maintenance of systems, the process follows established procedures of change management. Key security components related to these procedures includes:

- Identification and mitigation of possible risks
- Project and key contract security reviews to ensure security compliance
- Utilization of established change control processes to transfer changes from the development to the production environment.

Security requirements defined in GlobalConnect security governance are communicated, and responsibilities for implementation are delegated to the line organization, The line organization implements security measures in compliance with GlobalConnect governing documents.



Security Incident Management

GlobalConnect's Security Operation Center (SOC) is a centralized cyber security unit dedicated to prevent, detect, respond to and investigate security incidents. The SOC team manages a variety of services, which focus on security within customer's and GlobalConnect's network.

GlobalConnect has a documented incident response process which includes:

- Escalation process
- Pre-defined roles and responsibilities
- Cyberattack response plan

The SOC team provides operational support in all relevant security areas, and gives security guidance and awareness training. The SOC team is also responsible for leading internal IT forensics and investigations.

GlobalConnect maintains zero tolerance towards criminal activities. Measures are in place to detect and promptly respond to security incidents. All GlobalConnect personnel and line managers are obligated to report security incidents according to established routines.

Crisis Management and Continuity

GlobalConnect has an established crisis management organization in place at both group and country level to ensure the ability to promptly and decisively handle crisis. Crisis management plans enable the Crisis management teams to effectively manage and communicate the necessary information in an ongoing crisis.

Operations are continuously monitored by GlobalConnect's Network Operations Center (NOC). The NOC team monitors the status of the production environments and focuses on preventing incidents by initiating proactive measures. In case of an incident, the NOC team seeks to minimize the impact with minimal outage time for customers. The NOC team also manages information to customers, analyses production quality impact, identifies needed improvements, and inform stakeholders to ensure a high service quality.

GlobalConnect also maintains a Continuity Plan for its critical operations. The purpose of the plan is to provide a set of guidelines and procedures for supporting business processes in the event of a disasters i.e. fire, power outages, storms, floods, civil unrest.

Security Compliance

Security compliance verification is continuously conducted to ensure operational implementation of group security policies, instructions and directives in line with legal requirements, adopted international standards of best practice and contractual requirements.

To ensure compliance, GlobalConnect's security requirements, including review frequency, roles, mandate and responsibility, are defined and delegated to the line organization who is responsible for implementation and compliance. Security awareness training is regularly arranged to aid compliancy work within the organization.

Annual Security audits is determined, initiated and overseen by Group Security. Non-compliance is reported to the Group Chief Security Officer (Group CSO).