FIVE HOLDINGS

Development / Hospitality

DATA PRIVACY AND INFORMATION SECURITY

Data Privacy

FIVE follows the principles of data privacy and protection to ensure that personal information is collected lawfully, fairly, and transparently. Personal information is only collected for specific, clear, and legal reasons and is limited to what is necessary. FIVE also ensures that the personal information collected is accurate and kept up to date. The storage of personal information is limited to the duration necessary for its intended purpose. The company takes appropriate technical and organizational measures to protect personal information from unauthorized processing, accidental loss, destruction, or damage. Overall, FIVE adheres to the principles of data privacy and protection to safeguard personal information.

FIVE_Holdings_Data Privacy Policy.Pdf

Information Security

At FIVE we believe the preservation of confidentiality, integrity, and availability of systems and information used by an organization's members is critical and hence it is an integral part of the FIVE IT landscape. It defines the capabilities and requirements to protect information and systems from unauthorized access, use, disclosure, disruption, modification, data loss or destruction.

FIVE is committed to being transparent and ensuring fair and secure processing of any information relating to its employees, job applicants, external/third-party personnel including consultants, interns, and contractors in accordance with the data privacy laws in the countries it operates, industry-leading practices, and recognized international standards on privacy and the protection of personal information.

FIVE is certified to the ISO standards of 27001 – Information Security Management System which reflects the comprehensiveness of the information security management system including the process of risk assessments, structure and responsibilities, targets and objectives, trainings, physical and technical safeguards, incident management and audits. These aspects have been covered in the Information Security Policy.

FIVE's Information Security Policy constitutes the commitment of FIVE's management to take responsibility for achieving an organization-wide level of information security and setting a baseline for the information security controls that shall be applied by FIVE Holdings (BVI) Limited.

FIVE's Information Security Policy defines the authority, roles and responsibilities of Information Security and the personnel responsible for protecting FIVE resources.

FIVE HOLDINGS

Development / Hospitality

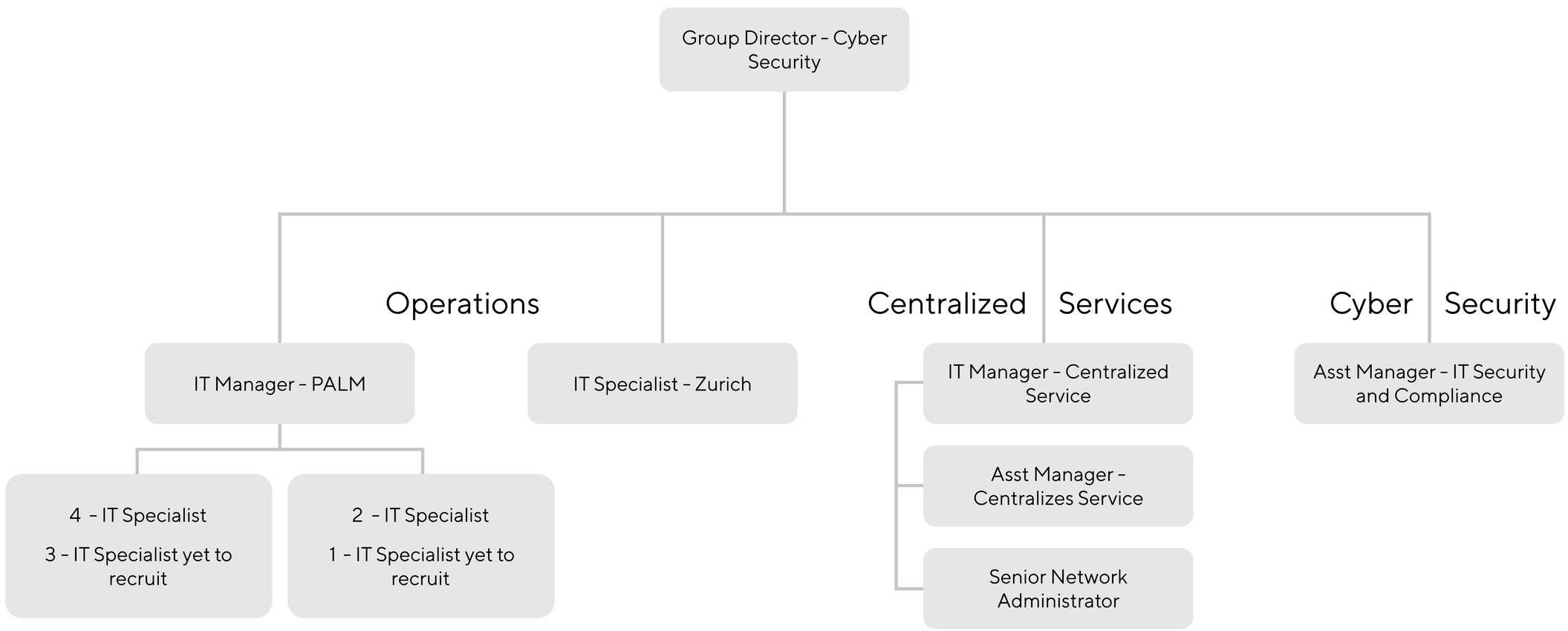
DATA PRIVACY AND INFORMATION SECURITY

The information security organization structure at FIVE shall consist of:

- Security Steering Committee (SSC)
- Group Director – Cybersecurity
- IT Security Compliance Officer
- Senior Management

Responsibilities of the information security organization structure are defined in the policy

IT Org Chart



IT Targets and KPIs

The FIVE organization aims to establish and maintain an information security awareness and training program to ensure that all users who have access to IT information assets understand their responsibilities and adhere to the information security policies in place. The organization plans to implement an organization-wide information security awareness and training program, with new users receiving training as part of their induction program.

To ensure that the information security awareness and training program remains up-to-date, the program material will be reviewed annually and updated to reflect any changes in FIVE's environment. The effectiveness of the security awareness and training program will be measured according to the Information Security Awareness and Training Procedure. Compliance with the program will be monitored and reported to the SSC on a quarterly basis.

FIVE HOLDINGS

Development / Hospitality

DATA PRIVACY AND INFORMATION SECURITY

KPI	Description	Target
Number of security incidents	The number of times a hacker – or several – has gained access or has	3 Nos
Time to detect and respond	This measures the time it takes for the organization to detect and respond	48 Hours
Vulnerability management	This measures how quickly vulnerabilities are identified and patched.	14 days
Security awareness training	This measures the effectiveness of the organization's security awareness	95% computer Users will cover
Compliance with security policies and regula	This measures the organization's compliance with internal security policies	100% compliance
Risk assessment and management	This measures the effectiveness of the organization's risk assessment and	90% of Risk Mitigation based on the project
Business continuity and disaster recovery	This measures the organization's ability to maintain business continuity	RPO - 24 Hours
System availability	This measures the time that IT systems are available for use by the	99% Uptime for Internal Applications
IT budget	This measures the amount of money allocated to IT and how it is being	90% of time within the budget
IT project success rate	This measures the percentage of IT projects that are completed on time,	90% of Time with in the target
IT staff productivity	This measures the productivity of IT staff. This KPI can be measured as the	90% of Time with in the target

IT Audit at FIVE

FIVE’s ensures periodic audit covers the assessment based on a test of the design and effectiveness of the Information Security Management System (ISMS) and the implemented security controls

FIVE_Information Secuirty Policy.Pdf