SUMMARY OF MOROIL'S INFORMATION TECHNOLOGY AND INFORMATION SECURITY POLICIES

25 April 2025

Introduction

The summary outlines the rules and guidelines that users within the organization or its networks need to follow to ensure the security of MOROIL's information, assets, and data to establish a secure environment and prevent unauthorized access, data breaches, and other cybersecurity incidents.

Policies Description Summary

No	Policy Name	Description
1	Change Management Policy	Designed to provide an orderly method in which changes to the production environment are requested and approved prior to the installation or implementation. The purpose is to question the rationale for the change, ensure that all elements are in place, the change plan is adequate, all parties are notified in advance, and the schedule for implementation is coordinated with all other activities within the organization. Most problems that occur in the production environment are the result of changes. The more successfully changes are controlled the more likely we are to minimize problems that arise as a result of changes.
2	Capacity Management Policy	Capacity management enables you to manage demand according to business priorities, so you can make sure that critical processes always have enough capacity to run effectively. It helps businesses with budgeting and scaling so they can identify their optimal levels of operations.
3	Antivirus Policy	It defines how antivirus is managed on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs.
4	Incident Management Policy	Process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, ensuring that agreed levels of service quality are maintained. The goal is to return to normal business operations as swiftly as possible by removing the threat, minimizing damage, and preventing similar incidents in the future

Policies Description Summary

No	Policy Name	Description
5	Back up and Restore Policy	A backup policy is a pre-defined, set schedule whereby information from business applications such as Microsoft SQL, email server databases and user files are copied to disk and/or tape to ensure data recoverability in the event of accidental data deletion, corrupted information or some kind of a system outage.
6	Logging and Monitoring Policy	It helps to speed up the process of identifying specific exceptions, when these exceptions occur and the frequency at which they occur. Additionally, it provides developers and support personnel with a greater level of visibility into the systems and applications being monitored. In the event of any incident, it helps to analyse for further investigation.
7	Software Asset Management Policy	It involves managing and optimizing the purchase, deployment, maintenance, utilization, and disposal of software applications within an organization. Also, it helps ensure that only license software are used and better at detect freeware which can ultimately caused business disruptions due to open ports and vulnerability.
8	Remote and Teleworking Policy	The aim of the policy is to provide appropriate remote access to employees, suppliers and contractors while protecting the information assets and systems from accidental or malicious loss or damage.

Policies Description Summary

No	Policy Name	Description
9	Mobile Device Policy	A mobile device management policy establishes rules for how mobile devices are used and secured within Moroil. Without mobile usage guidelines, we leave Moroil open to cybersecurity threats, theft and corporate espionage attempts.
10	Vulnerability Management Policy	A vulnerability management policy ensures that you're addressing the highest-risk vulnerabilities. Vulnerability management gives you a process and the tools to regularly identify and remediate your most critical and high-risk vulnerabilities.
11	Network Security Policy	A network security policy is a formal document that outlines the principles, procedures and guidelines to enforce, manage, monitor and maintain security on a computer network. It is designed to ensure that the computer network is protected from any act or process that can breach its security

Policies Description Summary

No	Policy Name	Description
12	Information Transfer Policy	An Information Transfer policy ensures and maintains the security of information transferred to any external entity or organization and secure information transfer within MOROIL.
13	BYOD Policy	BYOD policy is a policy that allows employees of MOROIL to use their personal devices for work-related activities. Those activities include tasks such as accessing emails, connecting to the MOROIL network, and accessing corporate applications and data.
14	Asset Management Policy	Asset management policy ensures the protection and preservation of all MOROIL owned assets. The Asset management policy will help MOROIL in better receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and dispositions are well known within MOROIL.
15	Information Classification Policy	The Information Classification Policy will help MOROIL determine what information can be disclosed to external parties and employees, as well as the relative sensitivity of information that should not be disclosed outside of MOROIL without proper authorisation. This policy also helps MOROIL to ensure that correct classification and handling methods are applied managed accordingly. MOROIL information assets should only be made available to all those who have a legitimate need to access them.

Policies Description Summary

No	Policy Name	Description
16	Media Handling and Disposal Policy	This policy is intended to guide and inform MOROIL personnel and help them understand their roles and responsibilities according to the policy. This policy ensures compliance with legal requirements to keep data secure while disposing of surplus information technology equipment containing data storage devices at MOROIL.
17	Risk Assessment Policy	The risk assessment policy defines the methodology for the assessment and treatment of information security risks within MOROIL, and to define the acceptable level of risk as set by MOROIL's leadership. Risk assessment and risk treatment are applied to the entire scope of MOROIL's information security, and to all assets which are used within MOROIL or which could have an impact on information security within it.
18	Access Control Policy	The access control policy ensures that controls are placed on both physical access to the MOROIL facilities and to MOROIL's information in order to limit and control access to computer networks and data of MOROIL.
19	Cryptography Policy	The Cryptography policy defines the encryption procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory, and contractual requirements within and to MOROIL facilities and information as well as its assets.

Policies Description Summary

No	Policy Name	Description
20	Physical and Environmental Control	The Physical Security and Environmental Controls Policy outlines measures to protect organizational premises, equipment, and information from unauthorized physical access, damage, or interference. It covers perimeter security, access control mechanisms (e.g., badges, biometric readers), visitor management, surveillance systems, and environmental controls such as fire protection, climate regulation, and uninterruptible power supplies. The policy ensures that access is restricted based on job roles and is regularly reviewed, and it mandates procedures for secure areas, equipment protection, and emergency response preparedness.
21	System Acquisition, Development and Maintenance Policy	The System Acquisition Development, and Maintenance policy cover controls for the identification, analysis, and specifications of information security requirements, securing application services in development and support processes, technical review restrictions on changes to software packages, secure system engineering principles, secure development environment, outsourced development, system security testing, system acceptance testing and protection of test data.
22	Third Party Security Policy	MOROIL uses third-party products and services to support the mission and goals. Third-party relationships carry inherent and residual risks that must be considered as part of the due care and diligence. The Third Party Security Policy defines the requirements for how MOROIL will conduct third party security due diligence.
23	Social media policy	This policy aims to protect Moroil’s reputation, sensitive information, and data as well as to regulate the appropriate and secure use of social media platforms by its employees and representatives while ensuring that social media activities align with the company's values, branding, and overall security strategy.

Policies Description Summary

No	Policy Name	Description
24	Information Security Incident Management Policy	The purpose of the incident management policy is to provide organization-wide guidance to employees on the proper response to, and efficient and timely reporting of, computer security-related incidents, such as computer viruses, ransomware, unauthorized user activity, and suspected compromise of data.
25	Human Resources Security Policy	The Human Resources Security Policy ensures that all employees (including contractors and any user of sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated. The policy also helps the MOROIL's employees in better understanding their roles and responsibilities towards information security practices at MOROIL.
26	Compliance Policy	The Compliance policy ensures that MOROIL comply with regulatory laws and obligations relating to the MOROIL activities. The policy also enables MOROIL's employees to work in an environment where they assume responsibility for compliance. The policy also assesses the existing compliance program and promote and implement continuous improvement of processes and procedures within MOROIL and develops and supports a culture of compliance within MOROIL.
27	Release and Patch Management Policy	The Release and Patch Management policy lists the guidelines and requirements for the proper management of vulnerabilities and involves various phases such as testing, deploying, and documenting the security patches applied to MOROIL's assets.

Policies Description Summary

No	Policy Name	Description
28	Internal SLA Policy	The internal SLA policy lets MOROIL set standards of performance for the support team. The internal SLA sets a target, or a deadline, within which the IT team is expected to respond and resolve tickets within MOROIL.
29	BCP-DRP Policy	BCP and DRP policy enables MOROIL in enabling and planning a MOROIL's business recovery of its critical business processes and IT systems in an efficient and timely manner in the event of any disaster.
30	Information Security Roles and Responsibilities Policy	The Information Security Roles and Responsibilities policy establishes the roles and responsibilities within MOROIL, which is critical for effective communication of information security policies and standards. These roles are required within MOROIL to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished.
31	Acceptable Use Policy	The Acceptable Use policy (AUP) outlines a set of rules to be followed by MOROIL employees while making use of any MOROIL information, assets or network. The Acceptable Use policy clearly states what MOROIL users are and are not allowed to do with MOROIL resources.
32	Information Security Policy	The Information security policy is a set of MOROIL information security policies which ensures that all information technology users within MOROIL or its networks comply with rules and guidelines related to the security of MOROIL's information, assets and data.

Policies Description Summary

No	Policy Name	Description
33	Artificial Intelligence Policy	The Artificial Intelligence (AI) Policy establishes controls for the ethical, secure, and compliant use of AI technologies within the organization. It covers governance of AI systems, data quality and bias mitigation, accountability and transparency of AI-driven decisions, security measures for AI models and data, compliance with applicable legal and regulatory frameworks, and the requirement for human oversight in critical use cases. The policy also includes provisions for risk assessment prior to AI adoption, monitoring of AI behavior, and incident response in case of AI system failures or misuse.
34	Operations Security Policy	The Operations Security Policy defines controls for the secure and reliable operation of IT infrastructure and services. It includes requirements for change management, capacity and performance monitoring, protection against malware, logging and monitoring of critical events, backup and recovery, secure disposal of media, segregation of duties, and protection of operational software and infrastructure. The policy also outlines roles and responsibilities for system administrators, incident response coordination, and ensures compliance with security baselines and standard operating procedures.