ENL Group

IT & Security Consolidated Policies

Version 4

Document Status	Final
Published Date	March 2023
Next Review Date	March 2024
Author(s)	ENL Corporate Services
Classification	Internal

Table of Contents

Executive Summary 3
1. Acceptable Use Policy 5
2. Risk Management Framework 5
3. IT Procurement and Vendor Management 6
4. Secure Software Development 6
5. Change Management 6
6. Security Management 7
7. Capacity and Configuration Management 7
8. Identity and Access Management 8
9. Patch Management 8
10. Physical and Environmental Security 8
11. IT Incident and Event Log Management 9
12. Backup and Restore 9
13. Resilience 10
14. Security Incident Response and Management 10
15. Removable Media 11

Executive Summary

Purpose

The purpose of the policies is to preserve confidentiality, integrity and availability of systems and information used by ENL and its subsidiaries.

- Confidentiality involves the protection of assets from unauthorised access.
- Integrity ensures the modification of assets is handled in a specified and authorized manner.
- Availability is a state of the system in which authorised users have continuous access to said assets.

The IT and Security Policies and Procedures is a document that must be continually updated to adapt to evolving business and IT requirements.

Applicability

The policies are aligned with the information security management systems standards published by the International Organization for Standardisation (ISO) set forth in ISO 27001 and 27002. The policies apply to ENL and its subsidiaries.

The Policy applies to the use of ENL information, information systems, devices and premises to conduct business or interact with internal networks and business systems, whether owned or leased by company, the employee, or a third party.

Enforcement and Compliance

1) Enforcement of the Policies is mandatory.
2) Compliance with the Policies is mandatory for all employees as per applicability. Depending on the type of IT system, the General Manager, Finance Manager, the Head of ICT, IT In-Charge or relevant Line Managers are responsible for ensuring compliance with the policies.
3) Compliance with the Policies is deemed part of the contract of employment for employees, contractual staff, consultants and through non-disclosure agreement entered by vendors and third parties.

Exceptions

1) Exceptions to be sought from Head of ICT or IT In-Charge and CISO for any deviations to the Policies based on adequate business justification and recommendation/approval by respective Business Division Head, unless otherwise outlined in specific policy in this document.
2) Head of ICT, IT In-Charge and CISO presents exceptions (if any) to the management for ratification.

Violation

1) Violations of the Policies, either by negligence or intentional, is subject to disciplinary actions as deemed fit by the ENL's management.
2) The disciplinary action results in a verbal/written warning, counselling, and revocation of access rights, termination of service/employment or a legal action, claims for compensatory damages, depending upon the severity.

Note

- The Board had ultimate responsibility for the group Information Technology and security at both strategic and operational level. The Board delegates the responsibility and authority to the General Manager for ensuring the effectiveness of the Group policies and procedures from a risk and strategic alignment perspective, as required by the Group Audit Committee.
- The General Manager has the broad overall responsibility to monitor the adequacy, efficiency and effectiveness of IT & security policies and procedures.
- The Head of ICT or IT in-charge is responsible for implementation, management, monitoring of policies and procedures.

1. Acceptable Use Policy

ENL demonstrates its commitment to information security by implementing policies and guidelines for the usage of ENL facilities and ENL information.

All ENL Personnel without exception are responsible for complying with ENL's Acceptable Use Policy (AUP). It is the responsibility of ENL and its subsidiaries to ensure that the information assets are protected from internal or external threats, whether deliberate or accidental, such that:

- Confidentiality of information is maintained.
- Integrity of information can be relied upon.
- Information is available when the business needs it.
- Relevant statutory, regulatory, and contractual obligations are met.
- The ENL brand and reputation is protected.

All Individual Users are responsible for exercising good judgment regarding appropriate use of the information and Information systems in accordance with group policies and standards, and local laws and regulation.

2. Risk Management Framework

ENL has established a Risk Management framework to identify potential threats to an organisation and to define the strategy for eliminating or minimising the impact of these risks, as well as the mechanisms to effectively monitor and evaluate the residual risks on an ongoing basis.

The objective of this framework is to:

- Identify and assess risk and threats in ENL IT ecosystem.
- Plan suitable responses to mitigate or avert potential risk and threats in ENL IT ecosystem.
- Protect ENL assets and systems by implementing security controls that support early risk detection and resolution.
- Preserve the confidentiality, integrity and availability of all information assets.
- Document risks in a continuously updated Risk Register

3. IT Procurement and Vendor Management

Through a well-defined IT procurement and vendor management approach, ENL ensures that risks can be minimized while bringing additional value and ensuring integration with the existing IT infrastructure of the group.

The purpose of this policy is to provide a framework for the procurement and management of vendors, with the objectives to:

- Ensure that procurement of IT goods and services is aligned to ENL and its subsidiaries' strategic objectives.
- Promote a consistent approach to procurement of IT goods and services across subsidiaries within the group.
- Facilitate integration of procured hardware and software within the group's IT infrastructure.
- Support procurement decisions with relevant information focusing on requirement fit and value for money.
- Ensure that products and services provided by vendors and service providers are governed by appropriate Service Level Agreements, warranties or maintenance contracts.

4. Secure Software Development

The group applies this policy during any software development process regardless in-house. ENL ensures that proper coding standards are followed by internal development or third-party suppliers and security assessment are performed on critical system prior to system going live.

The objective of this policy is to:

- Define requirements for in-house and client related software development process.
- Safeguard against unsafe coding practices which can result in costly vulnerabilities in application software that may go undetected and lead to unauthorised access, modification or destruction of data.
- Ensure effective management of the application development and change management processes with the implementation of appropriate controls throughout the system development lifecycle (SDLC).

5. Change Management

Changes to ENL IT systems are subject to a formal change management process that provides for a way by which such changes are requested, approved, communicated prior to implementation, logged and tested. The change management policy will help ENL to minimise risk and impact to its operations.

ENL has implemented a change management policy to:

- Ensure that requests for changes are supported by valid business and/or technical requirements.
- Evaluate the cost effectiveness of implementing the requested changes (for changes which have cost implications).
- Prevent or reduce the likelihood of unplanned disruptions to production IT systems.

6. Security Management

Security management enables ENL to protect its IT operations and assets such as network devices, databases, servers, user endpoints, mobility devices and cloud computing against internal and external threats, intentional or otherwise.

The objective of this policy is to:

- Ensure that there are sufficient security controls on ENL IT environment to protect its sensitive data.
- Ensure that all applications, data, business process assets and critical or important technology assets are secured and properly maintained.
- Ensure that the networks, devices and systems used to enable the operations of ENL and its subsidiaries are configured, secured and monitored accordingly.

7. Capacity and Configuration Management

Maintaining a high-performance and reliable IT environment is crucial to the operations of ENL IT infrastructure for establishing and maintaining consistency of IT performance, functional and physical attributes.

The purpose of this policy is to:

- Ensure that the required capacity exists within the IT environment.
- Ensure that IT services is provided in a cost-effective and timely manner.
- Facilitate changes in software and applications when they occur and establish system integrity and visibility.

8. Identity and Access Management

This policy facilitates the proper management and protection of information systems against unauthorised access, loss, contamination or destruction. ENL implements strong access controls to reduce the risk of accidental or deliberate modification or destruction of data as well as protecting against unauthorised access or dissemination.

The purpose of this policy is to:

- Secure information assets and information processing facilities of ENL through definition of rules for the creation, monitoring, control and removal of user access to IT assets and services based on the business requirements.
- Grant access to ENL information resources in a manner that carefully balances restrictions designed to prevent unauthorised access against the need to provide unhindered access to informational assets.

9. Patch Management

ENL defines the patch management policy to outline the security controls needed for patching, and to describe the patching controls and constraints for minimizing information security risks affecting ENL's digital assets.

The objective of this policy is to:

- Determine appropriate patched for software program and schedule installation of patches across different systems.
- Apply best practices when acquiring, testing and installing patches to administered computer systems.

1. Ensure systems bugs are fixed, up to date and protected against security vulnerabilities and bugs.

10. Physical and Environmental Security

Physical and environment security protects the building and related IT infrastructure supporting IT systems against physical and environmental threats. Additionally, environmental controls protect the IT infrastructure from damage due to natural or man-made threats.

ENL defines and implements the minimum physical security requirements and environmental conditions for facilities where IT infrastructure is stored to:

- Protect against common threats such as theft and damage.
- Avoid damage or unauthorised access to information and systems
- Automatic alert systems to inform the defined persons in order to react on a timely manner

11. IT Incident and Event Log Management

ENL recognises that IT incidents are disruptive and can have a severe operational impact on clients or the business function. The Incident and Event Log Management Policy facilitate the identification, classification, escalation and response to incidents in a timely manner and reduce impact to the individuals and the business.

ENL's aim is to:

- Define a consistent process across entities within the group.
- Address incidents as quickly as possible or within agreed service levels to minimise impact on normal operations.
- Be prepared to combat threats and quickly respond to prevent impacts that may result in financial, legal or reputational implications.
- Ensure that all incidents and problems are documented for future reference and analysis.
- Manage the expectations of end-users.
- Identify and address the underlying causes of recurring incidents so as to implement permanent solutions and avoid future cost.

12. Backup and Restore

ENL applies best practices for making periodic copies of data and applications to a separate secondary device and then using those copies to recover the data and applications that business operations are dependent on.

ENL implements this policy to:

- Ensure that all business data is backed up as per business requirements and is recoverable within an acceptable time frame following a disruption.
- Data can be recovered in the event that the original data are lost or damaged due to a power outage, cyberattack, human error, disaster or some other unplanned event.

13. Resilience

ENL provides a holistic management process that identifies potential threats that may disrupt critical business operations, with the framework for building resilience and establishes the capability for effective response to safeguard the interests of stakeholders.

This policy helps ENL to prepare with an effective Business Continuity Management (BCM) and Disaster Recovery Plan (DRP) to respond in case of business disruption or crisis.

The aim of this policy is to establish and sustain a business continuity management framework to:

- Enable the continuity of business if there is a loss of staff, facilities, information systems or data in a Business Continuity Plan.
- Protect the people and assets of companies within the group in a Disaster Recovery Plan.
- Raise awareness of business continuity management.
- Manage crises and minimise ensuing disruptions to critical business activities in a Crisis Management Plan.
- Ultimately protect value creating activities, reputation, and brand.

14. Security Incident Response and Management

ENL depends on the confidentiality, integrity, and availability of its information to successfully conduct its business, meet consumer and business partner expectations. ENL recognises the existence of threats from internal users or external stakeholders to intentionally or unintentionally breach ENL's security through events such as but not limited to unauthorized access, malware, improper privilege escalation loss or theft of ENL assets or email compromise.

In order to minimize the potential impact of such an event occurring, ENL shall respond quickly and effectively. The Security Incident management policy provides general procedures on how to identify and handle incidents that affect the confidentiality, integrity and availability of information of ENL. It defines the roles and responsibilities and procedural steps that designated ENL staff should take when responding to incidents.

ENL's aim is to:

- Establish a clear definition of what constitutes a security incident and identify the team or individuals responsible for identifying and reporting incidents.
- Determine the severity of the incident, categorize it based on its potential impact, and prioritize the response accordingly.
- Establish a clear communication plan to notify relevant parties of the incident, including internal stakeholders and external regulatory bodies if necessary.

- Take immediate steps to contain the incident to prevent further damage, including isolating affected systems, shutting down compromised accounts, and blocking network traffic.
- Conduct a thorough investigation to determine the root cause of the incident, the extent of the damage, and any potential vulnerabilities that may have been exploited.
- Develop and implement a plan to restore affected systems and data to their pre-incident state.
- Conduct a post-incident review to identify lessons learned and make necessary improvements to the incident response plan to prevent future incidents.

15. Removable Media

ENL applies a least-privilege principle with regards to removable media. ENL, by default, restrict the use of removable media devices on company-managed devices.

The aim of this policy is to:

- Minimise the risk of data breaches due to unauthorised transfer of sensitive information to a removable media.
- Minimise the risk of malware infections using removable media as an infection vector.
- Define the limited and authorised use of removable media devices for business activities.
- Provide a brief for requests for elevated privileges with respect to removable media usage.