IT security policy

Version: 1.0 April 2024

POLICY NAME	IT security policy
POLICY MANAGER	Executive General Manager, Group Quality, Accreditation & Compliance
APPROVAL AUTHORITY	CEO
RELEASE DATE	April 2024
VERSION REFERENCE	Version 1.0 - New policy

Contents

1. Introduction

1. Purpose

The purpose of this policy is to set out the security principles to ensure the protection of NextEd Group Limited (NextEd) information and communication systems against unauthorised access, use, disclosure, modification, perusal, inspection, recording or destruction throughout their lifecycle.

2. Scope

This policy is an overarching Group policy and applies to:

i) All staff of NextEd including employees and contractors;
ii) All courses delivered by NextEd including those delivered on their behalf by education providers with whom there is a licensing arrangement. If there are any discrepancies between an affiliate's policy and these, the NextEd policy will apply.
iii) All students attending NextEd colleges.

3. Definitions

Word/Term	Definition
Business continuity plan	A business continuity plan (BCP) is a system of prevention and recovery from potential threats. The plan ensures that personnel and assets are protected and can function quickly in the event of a disaster.
Disaster recovery plan	A disaster recovery plan (DRP) Is a documented, structured approach to help to resolve data loss and recover system functionality so that it can perform in the aftermath of an incident, even if it operates at a minimal level.
NIST 800-63	The Special Publication (SP) 800-63 suite provides technical requirements for USA federal agencies implementing digital identity services. The publication includes: an overview of identity frameworks; using authenticators, credentials, and assertions in a digital system; and a risk-based process to select assurance levels.
Student	Means a student who is: • enrolled in a course delivered by a NextEd college; or • enrolled in a course offered by an entity operating on behalf of NextEd.

2. Policy

1. Policy

a. NextEd is committed to protecting its information and communication systems against unauthorised access, use, disclosure, modification, perusal, inspection, recording or destruction. All practices concerning information assets within NextEd are to be in accordance with this policy, and supporting procedures in order to safeguard the confidentiality, integrity and availability of NextEd's information assets.

b. All relevant statutory, regulatory, and contractual requirements and NextEd's approach to meet these requirements will be defined, documented, and kept up to date.

c. Regulatory reports will be submitted as requested by regulators including the Australian Securities Exchange (ASX) and the Australian Securities and Investment Commission (ASIC)and other government regulators as and when required.

d. NextEd will strive to identify and assess all reasonable foreseeable security related hazards.

e. The General Manager - IT will develop IT security control strategies and implement these strategies for any identified security related hazard to reduce risk. These strategies will form part of the information security management system and be published and communicated to all employees and relevant parties.

f. The IT team will regularly review the status of IT security at NextEd.

g. The General Manager - IT will approve any IT security projects, approve new or modified IT security procedures and perform other necessary high-level IT security management activities.

h. Requirements for confidentiality or non-disclosure agreements reflecting NextEd's needs for the protection of information will be identified and regularly reviewed.

i. The approach to manage information security and its implementation may be reviewed by persons external to IT Operations, at planned intervals or when NextEd implements significant security changes.

2. Information security management system

a. Security control requirements for assigning and authorising access to NextEd's information and communication systems will be defined and implemented in line with business requirements.

b. Procedures will be developed and implemented that minimise the risk, loss or misuse of information and communication systems by ensuring security responsibilities are incorporated and communicated during recruitment, termination or change of employment within NextEd.

c. Appropriate security controls will be implemented to protect NextEd's information assets from digital, physical, and environmental threats. Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorised access to information and to protect against loss or damage.

d. Procedures and security controls will be appropriate to the value and criticality of the information and communication system or information asset.

e. Operating procedures and roles and responsibilities will be documented, maintained, and made available to all users who need them, to enable all information and communications systems to be managed securely and consistently.

f. Procedures will be established to ensure that security events will be reported through appropriate management channels and responded to as quickly as possible including compliance with legal requirements.

g. A BCP and a DRP will be maintained to help maintain security in the face of unexpected events and changes by ensuring critical functions continue to operate when a system is working in a degraded state or reducing the time between when a disaster occurs, and critical functions being restored.

3. Access control

a. Control requirements for assigning and authorising access to NextEd's information and communication systems are defined and implemented in line with business requirements and consistent with policy and legal requirements.

b. Authentication controls mechanisms should be as a minimum authorization, authentication, access rights approval, and audit based upon risks associated with the information asset.

c. The processes for managing access rights are to be reviewed at least annually to ensure they remain appropriate.

d. This policy applies to access controls for:

   a. Networks

   b. Operating systems

   c. Applications

   d. Information

4. Passwords

a. Employees must not share passwords and keep passwords secure at all times.

b. Employees should lock or log off from IT systems before leaving them unattended.

c. All passwords are required to meet the standard of NIST 800-63 for password security.

d. To minimise security risks to information or communication systems appropriate control mechanisms need to be in place that include:

   a. rules for creating effective passwords and for regular changing of passwords,

   b. systems to test the security of passwords,

   c. firewalls and filters,

   d. classification and transmission protocols for business records,

   e. regular risk assessments,

   f. monitoring the use of information and communication systems,

   g. compliance with the appropriate sections of the Security Standard AS/NZS ISO/IEC 27002 as it applies to the secure transmission of personal health information, and

   h. providing personal access points, including computers, with time-based locking mechanisms, which are password activated.

5. User accounts

a. To ensure that all information systems, networks and applications can uniquely identify and restrict the privileges of each user, unique user-identifications will be assigned to each user to carry out their role-based function with NextEd. User-identifications will be decommissioned when the user ceases their employment with NextEd.

b. Access to information and communication systems will be granted to specific individuals, and not generic user accounts or administrative accounts.

c. The creation of generic system accounts for information and communication systems will be reviewed and approved by the General Manager - IT to confirm the need for and the correct credentials are applied and control mechanisms are in place to prevent incorrect use.

d. The information and communication system privileges of all users, systems and programs must be restricted based on the principles of least privilege. This is defined as the minimum access necessary to perform the required functions of the role (role-based access).

e. Role-based access will be used across all development, test, and controlled production environments to reduce the risk of unauthorised access or changes to operational systems. These role-based access privileges will be revoked if the user changes roles.

f. To ensure proper separation of duties, IT will define role-based access privileges such that ordinary users cannot gain access to, or otherwise interfere with the individual activities or the private data of other users.

g. Formal registration, approval and de-registration procedures will be in place for granting and revoking any access to information and communication systems. Third party access control must be supported by a signed confidentiality agreement.

h. Elevated role-based access for system privileges will be restricted to those directly responsible for system management or security and must be approved by the General Manager - IT or delegate.

i. The role base access privileges granted to every user must be re-evaluated at least annually to ensure that enabled access privileges are appropriate to perform the functions of their current role.

6. System monitoring

a. NextEd reserves the right to track access to any network, application, or device.

7. Backup

b. Regular backups of essential business information must be taken to ensure that the organization can recover from a disaster, media failure or other form of error.

c. An appropriate backup cycle must be designed and used that meets business requirements, complies with the NextEd information security management system, and is fully documented. Third parties that store organisation information must also be required to ensure that the information is backed up appropriately.

d. In a cloud environment where the cloud service provider (CSP) is responsible for backups, the following criteria must be defined and agreed:

   a. Scope, schedule, and location of backups
   b. Backup methods and data formats
   c. Retention periods for backups
   d. How the integrity of backups will be verified
   e. Restoration and testing procedures, including restoration timescales during a disruptive event
   f. Use of encryption
   g. How backups are segregated in a multi-tenant cloud environment
   h. Frequency and method of reviews of backup and recovery procedures

e. Full documentation of the recovery procedure associated with each backup must be created and stored.

f. Regular restores of information from back up media must be performed to verify the reliability, accuracy, and integrity of the back-up media and the restore process.

3. Reference and Supporting Information

1. Supporting Documentation

Document name	Document type	Location
ISO/IEC 27001	Govt Standards	External
ISO/IEC 27002	Govt Standards	External
NIST 800-63	American Govt Standard	External
The Privacy Act 1988	Govt Legislation	External
Health Records and Information Privacy Act 2002 (NSW)	Govt Legislation	External
Health Records Act 2001 (Vic)	Govt Legislation	External
Cybercrime Act 2001	Govt Legislation	External

2. Change History

Version	Approval date	Approved by		Change
V1.0		Group Quality, Accreditation & Compliance	Group Manager	Development of Group Policy replacing existing entity level policies
		Office of Chief Executive	CEO	