IT Security Policy

IT SECURITY			
Effective Date	June 1, 2023	**Policy Type**	Administrative
Responsibility	Vice President Corporate Services (policy owner) Director, IT (policy manager)	**Related Policies**	IT Governance Passwords Acceptable Use Privacy/Disclosure
Approval Authority	Executive Council	**Review Schedule**	June 1, 2028

1. Policy Statement:

We are committed to protecting our assets, including data, hardware, and software, from unauthorized access, use, disclosure, and destruction. To achieve this, we have implemented an IT security policy that outlines our approach to managing IT security risks.

2. Scope:

This policy covers all systems user's as well as all organizational assets connected to information technology systems, networks, software, and data.

3. Reason for Policy:

The purpose of this IT security policy is to describe how legislation, regulation, and industry best practice relates to the standard operating procedures used the protect the organization's information and technology assets from unauthorized access, theft, damage, or loss. The policy outlines the responsibilities and expectations of all employees, contractors, and vendors regarding the security of our IT resources.

4. Guiding Principles and Policy

NWP is committed to protecting our IT resources and information from unauthorized access, theft, damage, or loss. To achieve this, we follow the following guiding principles:

5.1 Risk management: We regularly assess the risks associated with our IT resources and take proactive measures to mitigate those risks. This includes implementing security controls,

conducting regular security audits, and staying up to date with the latest security threats and vulnerabilities.

5.2 Compliance: We comply with all applicable laws and regulations regarding the protection of information and IT resources. We also adhere to industry-specific standards and best practices to ensure the highest level of security.

5.3 Continuous improvement: We strive to continuously improve our IT security measures to stay ahead of evolving threats and vulnerabilities. This includes regularly reviewing and updating our security policies and procedures, as well as providing ongoing training and education to our employees.

5.4 Collaboration: We recognize that IT security is a shared responsibility and require the active participation of all employees, contractors, and vendors. We encourage open communication and collaboration to ensure that everyone is aware of their responsibilities and understands the importance of IT security.

5.5 Confidentiality: We are committed to protecting the confidentiality of our information and IT resources. We restrict access to sensitive data and implement encryption and other security measures to ensure that it cannot be accessed by unauthorized individuals.

5.6 Availability: We strive to ensure that our IT resources are available to authorized users when they need them. This includes implementing backup and disaster recovery plans to ensure that critical data and systems are available in the event of a disaster or system failure.

By following these guiding principles, we can ensure that our IT resources and information are protected to the highest possible standard, reducing the risk of security breaches, and maintaining the trust of our stakeholders.

5.7 Access controls: Access controls are implemented to ensure that only authorized personnel have access to the organization's resources. This includes password policies, two-factor authentication, and access controls for physical assets such as servers and data centers.

5.8 Responsible Use: IT personnel is granted elevated access to perform their duties in support of the organizational goals. Anyone found accessing data or information in an unethical manner is subject to progressive discipline within the terms of their employment and any professional organizations to which they belong.

5.9 Monitoring and auditing: Monitoring and auditing systems should be implemented to detect and prevent security breaches. This can include logging, intrusion detection systems, and regular security audits. IT will take measures to respond to an immediate threat to the critical infrastructure, data, or persons.

5.9.1 Emergency: The Director, IT or designate has the authority to declare an IT emergency to protect the loss or damage of critical data or infrastructure, regardless of the disruption to regular institutional operations.

5.10 Training and awareness: Employees receive training on the risks and issues related to security procedures, and best practice, as well as their responsibilities for protecting data and systems.

6. Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Executive Council	• Approve and formally support this policy.
Vice-President, Administration	• Review and formally support this policy.
Director, Information Technology	• Develop and maintain this policy. • Review and approve any exceptions to the requirements of this policy. • Take proactive steps to reinforce compliance for all stakeholders.
Manager, Information Technology	• Implement the standard operating procedures in keeping with the requirements of this policy.
Manager, Enterprise Risk	• Maintain the IT Risk Register.
Audit Compliance Officer	• Coordinate with external auditors.
Supervisors or Institution Representative	• Support all employees and students in understanding the requirements of this policy. • Immediately assess and report to the IT Help Desk any non-compliance instance with this policy.
Contract Administrators	• Ensure that the password responsibilities and obligations of each party to the contractual relationship are outlined in the contract between the Institution and the contractor/sub-contractor.
All users (Employees and contractors, Students, Visitors and/or Volunteers)	• Comply with the requirements of this policy. • Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor, or Institution Representative as soon as possible.

7. **Definitions:** This section defines terms specific to this policy.

"Access Control" is the process that limits and controls access to resources of a computer system.

"System Users" are students, employees, consultants, contractors, agents, and authorized users accessing NWP IT systems and applications.

"System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications.

"Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.

"Access Privileges" are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

"Administrator Account" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.

"Application and Service Accounts" are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.

"Nominative User Accounts" are user accounts that are named after a person.

"Non-disclosure Agreement" is a contract between a person and the Institution stating that the person will protect confidential information (as defined in the Record Classification and Handling Policy) covered by the contract, when this person has been exposed to such information.

"Information Security Incidents" are unplanned events which affect the confidentiality and integrity of data and the availability of IT systems. Examples of an information security incident include: confidential data breach, privacy breach, unauthorized access to applications and network, malware contamination, web site defacement, etc. Security incidents that have a high probability of being exploited and that will highly impact the Institution (i.e. risk of operation disruption, data breach, etc.) are often labeled as "Critical" or "High".

"Critical Security Incidents" are security incidents that present the highest probability of being exploited and that have a high impact to the Institution.

"Information Security" is the practice of ensuring that information assets, as well as the technology systems that process, transmit or store such assets, are protected against threats that can affect them. This includes a comprehensive set of controls that cover various factors (human, physical, environmental, and technical) across the lifecycle of information and technology assets, including developing or creating new data or systems, maintaining data and systems, monitoring the use of such assets, detecting and reacting to potential attacks, complying with applicable cyber security and privacy laws and regulations, as well as decommissioning and destroying data and IT systems.

"Confidentiality" is the status of an information asset, or similarly a technology asset processing such information, relative to the secrecy or privacy of such information (i.e. whether the information asset can be shared with the general public or restricted to only a few authorized persons).

"Integrity" is the status of an information asset, or similarly a technology asset processing such information, relative to the completeness and unchanged aspect of such information (i.e. whether this information can be modified or not at any time or by any person).

"Availability" is the status of an information asset, or similarly a technology asset processing such information, relative to availability of access in a timely manner to the asset (i.e. whether this asset needs to be readily accessible at any time or can be accessed after a longer period of time).

"Emergency" refers to a critical situation or event in which an organization's IT systems, infrastructure, or services are disrupted or compromised, and immediate action is required to restore normal operations. IT emergencies can occur due to a variety of reasons, including hardware or software failures, cybersecurity attacks, natural disasters, power outages, or human errors. The severity of an IT emergency can range from minor issues that affect a single user to major incidents that impact the entire organization. Rapid and effective response is essential in managing IT emergencies to minimize the impact on business operations and prevent any further damage to the IT systems.

"Risk" refers to the potential negative impact on an organization's IT systems, infrastructure, or operations. It arises from the possibility of events, actions, or circumstances that can lead to the loss, corruption, or theft of data, disruption of services, or financial loss.

8. Review

April 13th, 2023
August 25, 2023 (minor edits)

References:

NIST Security Policy Framework Template
SANS Server Security Policy
SANS Web Application Security Policy