



THE COUNCIL OF LEGAL EDUCATION
THE NORMAN MANLEY LAW SCHOOL

User Security Awareness and Training Policy (USATP)

Table of Contents

DEFINITIONS.....	1
1.0 TITLE: User Security Awareness and Training Policy	1
2.0 POLICY STATEMENT	1
3.0 PURPOSE.....	1
4.0 SCOPE	2
4.1 Applicability	2
5.0 PROCEDURE.....	2
6.0 RESPONSIBILITY	3
6.1 Compliance/Monitoring/Review.....	3
6.1.1 Reporting.....	4
6.1.2 Records Management.....	4
7.0 ASSOCIATED DOCUMENTS	5
8.0 APPROVAL	5
9.0 APPENDIX.....	5


DEFINITIONS

Information Asset	An information asset is a body of information, defined and managed as a single unit so that it may be understood, shared, protected and used efficiently. It has a recognisable value, risk, context, and life cycle and may include personal data as defined in the DPA.
Information Technology	Systems (especially those related to computers and telecommunication) for processing data.
Information Security	The preservation of the confidentiality, integrity and availability of information whether in a physical or digital form.

Table 1. List of Acronyms/ Abbreviations

Initialisms/Acronyms	Meaning
DPA	Data Protection Act, 2020
IT	Information Technology
NMLS	The Council of Legal Education – Norman Manley Law School

NORMAN MANLEY LAW SCHOOL

	DEPARTMENT: Human Resources Department	DOCUMENT NO: HRD/USATP/01	Page 1 of 5
	TITLE: User Security Awareness and Training_ Policy (USATP)	REVISION NO.: 00	REVISION DATE: March 13, 2025

1.0 TITLE: User Security Awareness and Training Policy

2.0 POLICY STATEMENT

This policy details the provision of end user data protection awareness training and associated services throughout the organisation, designed to help build and maintain a positive security culture in relation to information security, data protection, risk and privacy.

The Information Assets of the Council of Legal Education - Norman Manley Law School (NMLS) are critical to its operational and strategic activities and all efforts must be taken to ensure these are protected from events that could cause disruption or jeopardise the integrity of its systems or data.


NMLS recognises that technical IT security measures form a vital part of our overall information security framework but are not, in themselves, sufficient to protect data alone. NMLS recognises that effective information security also requires the development of a positive security culture, ensuring end users are aware of their responsibilities as well as the types of attacks that they may be subjected to.

3.0 PURPOSE

3.1 By undertaking a programme of security awareness training, the NMLS can empower end users to recognise and react appropriately to information security threats and incidents, significantly reducing the risk of a physical or cyber-incident due to human error or through a lack of awareness.

3.1.1 NMLS is committed to complying with its statutory duty under data protection legislation, not only so that the organisation can avoid data breaches (which can help prevent possible fines and damage to its reputation) but also so that it can meet its obligations (both legally and morally) to any data subjects for whom NMLS holds and processes the personal data of (including, but not limited to, students, employees,

NORMAN MANLEY LAW SCHOOL

	DEPARTMENT: Human Resources Department	DOCUMENT NO: HRD/USATP/01	Page 2 of 5
	TITLE: User Security Awareness and Training_ Policy (USATP)	REVISION NO.: 00	REVISION DATE: March 13, 2025

clients, customers and suppliers). The implementation of user security awareness and training forms an important part of the organisation's efforts to achieve this.

4.0 SCOPE

4.1 Applicability

This policy applies throughout the organisation as part of our information security framework and applies regardless of an end user's role within our organisation.

Participation under this policy is mandatory.

5.0 PROCEDURE


The User Security Awareness and Training Procedures and reporting mechanisms will be communicated to all relevant personnel and reviewed annually.

Security Awareness Training

This relates to the education and training of persons and may cover:

- a) The nature of sensitive material and physical assets
- b) responsibilities in handling sensitive information, including nondisclosure and confidentiality agreements.
- c) Requirements for handling sensitive material in physical form, including transformation, storage, and destruction.
- d) Proper methods for protecting sensitive information on computer systems, including password policy and two-factor authentication.
- e) Other computer security concerns include malware, phishing, and social engineering.
- f) Workplace security, including building access, wearing of security badges, reporting of incidents, and forbidden articles.
- g) Consequences of failure to properly protect information, including the potential loss of employment, disciplinary procedure, economic consequences to the organisation, damage of individuals whose private records are time divulged and possible civil and criminal penalties.

NORMAN MANLEY LAW SCHOOL

	DEPARTMENT: Human Resources Department	DOCUMENT NO: HRD/USATP/01	Page 3 of 5
	TITLE: User Security Awareness and Training_ Policy (USATP)	REVISION NO.: 00	REVISION DATE: March 13, 2025

The organisation will provide security awareness training which will expose employees to the necessary knowledge and skills for safeguarding the information used during the course of their duties (and, indeed, during their personal lives also).

- a) All employees are required to participate in and complete security awareness training. For new hires, this training will be completed during the probationary period. Sensitisation and awareness training will be scheduled for employees periodically as needed to ensure they are kept abreast of changes in the information security landscape that impact operational activities.
- b) If a user fails to complete their respective security awareness training, the following actions will be implemented:
 - o HR will be informed of non-compliance and or;
 - o Supervisor/manager with responsibility for the users will be informed, and a specific action will be set to resolve the outstanding training.
 - o If the above actions fail to resolve the outstanding training, IT personnel will restrict the end user's account to prohibit access until training is completed satisfactorily, and the NMLS will determine the appropriate action to be taken in all the circumstances.

Where applicable:


- o User completion will be linked with the end user's performance review and a failure to complete the training may result in a lower performance grade being awarded.

6.0 RESPONSIBILITY

6.1 Compliance/Monitoring/Review

6.11 Policy Review and Maintenance

NORMAN MANLEY LAW SCHOOL

	DEPARTMENT: Human Resources Department	DOCUMENT NO: HRD/USATP/01	Page 4 of 5
	TITLE: User Security Awareness and Training_ Policy (USATP)	REVISION NO.: 00	REVISION DATE: March 13, 2025

This policy will be reviewed and updated every three (3) years or sooner as may be required to ensure it remains appropriate in light of changes to legislation, operational requirements or contractual obligations.

6.12 Responsibilities and Accountabilities

End Users:

It is the responsibility of all end users to ensure that they use the organisation's information and information systems appropriately, in accordance with the guidance provided with our associated policies.

Supervisor/Managers:

It is the responsibility of all Supervisors/Managers to ensure that end users for whom they have responsibility are aware of their responsibilities under this policy and to ensure that they complete each of the security awareness training modules allocated to them.

6.13 Contractors and Third Parties

Any contractors or third parties who access, use, or manage the organisation's information or information systems are responsible for coordinating and implementing relevant awareness and training courses for themselves and their employees. We would recommend that all such contractors or third parties seek their own programme of security awareness training.


6.1.1 Reporting

The Human Resource Manager is responsible for ensuring the effective implementation of the security awareness training programme and is accountable to the principal.

6.1.2 Records Management

Sufficient records shall be maintained by the NMLS to confirm the relevant training exercises which have been held on an annual basis in addition to the participants in such training exercises.


NORMAN MANLEY LAW SCHOOL

	DEPARTMENT: Human Resources Department	DOCUMENT NO: HRD/USATP/01	Page 5 of 5
	TITLE: User Security Awareness and Training_Policy (USATP)	REVISION NO.: 00	REVISION DATE: March 13, 2025

7.0 ASSOCIATED DOCUMENTS

- a) NMLS Data Protection Policy

8.0 APPROVAL

Current Document Revision #:	Rev 00
Revision Date:	March 13, 2025
Procedure Owner:	HR Manager
Approval Authority & Date:	 20/3/2025
Next Revision Date/Period:	March 2028
Document Revision Note:	

Revision History

Last Revision #:	
Last Revision Date:	
Change Summary:	

9.0 APPENDIX

None