THE COUNCIL OF LEGAL EDUCATION
THE NORMAN MANLEY LAW SCHOOL

The Norman Manley Law School Policy on the Use of Encryption

Table of Contents

20/3/2025

DEFINITIONS

Table 1. Key Terms and Definitions

Key Terms	Definitions
Algorithm	An algorithm is a set of commands that must be followed for a computer to perform calculations or other problem-solving operations. It is a systematic procedure that in a finite number of steps produces an answer to a question or the solution of a problem.
Application[i]	A programme, or group of programmes, hosted on enterprise assets and designed for end-user. Applications are considered a software asset in this document. Examples include web, database, cloud-based and mobile applications.
Ciphertext	is a result of encryption performed on plain text using a cipher. A cipher is a mathematical function that scrambles data so that it cannot be read by anyone who does not have the key to decrypt it. Cipher text is also known as encrypted or encoded information
Cloud environment	A virtualised environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
Cryptography[ii]	Cryptography is the practice of developing and using coded algorithms to protect and obscure transmitted information so that it may only be read by those with the permission and ability to decrypt it.
Cryptographic Keys[iii]	A cryptographic key is a piece of information that is used in combination with an algorithm to transform plaintext into ciphertext (encrypted text) or vice versa.
Data Authenticity	The property that data originated from its purported source[1]
Decryption	Decryption is the process of converting previously encrypted data into information that can be read by humans and/or computers.

20/3/2025

Key Terms	Definitions
Encryption[iv]	Encryption is the process of transforming readable plaintext into unreadable ciphertext to mask sensitive information from unauthorised users. The process of converting data into a code (ciphertext) to prevent unauthorised access.
End-user devices	Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones and tablets, as well as desktops and workstations. For the purpose of this document, end-user devices are a subset of enterprise assets.
Mobile end-user devices	Small, enterprise issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile end-user devices are a subset of portable end-user devices, including laptops, which may require external hardware for connectivity. For the purpose of this document, mobile end-user devices are a subset of end-user devices.
Network Infrastructure	Refers to all the resources of a network that make network or internet connectivity management, business operations and communication possible. It consists of hardware and software, systems and devices, and it enables computing and communication between users, services, applications, and processes. Network Infrastructure can be cloud, physical or virtual.
Non-Repudiation [v]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Physical environment	Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network.
Plaintext[vi]	Intelligible data that has meaning and can be understood without the application of decryption. It is ordinary readable text.
Portable end-user devices	Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this document, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets.
Remote devices	Any enterprise asset capable of connecting to a network remotely, usually from public internet. This can include enterprise assets such as end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers.
Removable media	Any type of storage device that can be removed from a computer while the system is running and allows data to be moved from one system to another. Examples of removable media include compact discs (CDs), digital versatile discs (DVDs) and Blu-ray discs, tape backups, as well as diskettes and universal serial bus (USB) drives.

20/3/2025

Key Terms	Definitions
Servers	A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers.
Technical and organisational measures	.
User accounts[vii]	An identity created for a person in a computer or computing system. It is an established relationship between a user and computer, network or information service. For personal computers there are typically two types of user accounts: standard and administrator. User accounts with escalated privileges are covered under administrator accounts.
Virtual environment	Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualised environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualisation is a fundamental technology that allows cloud computing to work.

Table 2. List of Initialisms/Acronyms

Initialisms/Acronyms	Meaning
LAC	**Legal Aid Clinic**
NMLS	The Council of Legal Education – Norman Manley Law School
DPA	The Data Protection Act, (2020)
DPIA	Data Protection Impact Assessment

20/3/2025

NORMAN MANLEY LAW SCHOOL

	DEPARTMENT/UNIT: Office of the Principal	DOCUMENT NO: OOP/ /UEPPro/ 00	PAGE 1 OF 29
	TITLE: The Use of Encryption Policy and Procedure (UEPPro)	REVISION NO.: 00	REVISION DATE: March 20, 2025

1.0 TITLE: The Use of Encryption Policy and Procedure

2.0 POLICY STATEMENT

In compliance with the seventh standard of the Data Protection Act, 2020 (DPA) The Council of Legal Education - Norman Manley Law School ("NMLS") is required to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data. The NMLS is committed to identifying and implementing appropriate cybersecurity measures to ensure compliance. For the purposes of the DPA, technical and organisational measures include the encryption of personal data.

3.0 PURPOSE

The purpose of this policy is to ensure that the NMLS employs measures to mitigate against accidental loss, destruction or damage of the personal data processed in its operations. The policy defines rules for the management of its internal technological systems and applications which include using encryption controls, and cryptographic keys, in order to protect the confidentiality, integrity, authenticity and non-repudiation of information. Encryption controls refer to measures implemented to secure data by converting it into an unreadable format through encryption algorithms. These controls ensure that only authorised individuals or systems can access and decrypt the data, protecting it from unauthorised disclosure or manipulation.

4.0 SCOPE

The policy applies to all network infrastructure, communication and storage devices used by the NMLS to manage information. This includes systems used to manage human resources, student information and Legal Aid Clinic (LAC) client and library user files. Whether held internally or managed by NMLS data processors, it extends to data on end-user devices containing sensitive data, data in transit, data at rest, data on removable media and cloud services.

20/3/2025

5.0 PROCEDURE

5.1 Use of Encryption

NMLS must ensure that the technical and organisational measures implemented provide a level of security appropriate to any harm that might result from such unauthorised or unlawful processing or accidental loss, destruction, or damage to the nature of the personal data to be protected.

Technical and organisational measures include :

a) pseudonymisation and encryption of persona data,
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
c) the ability to restore the availability of and access to personal data promptly in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing and;
e) measures to ensure the adherence to the technical and organisational[viii][2] requirements specified in the of the provisions of the Data Protection Act.

Based on the foregoing, NMLS must protect individual systems and information using the following encryption controls.

5.1.1 Encryption Controls

The Information Technology personnel are responsible for preparing detailed instructions on the use of the mentioned encryption tools. Owners of individual assets to which encryption controls are applied are responsible for appropriate application of individual encryption controls.

20/3/2025

[2] Section 30(6) of the Data Protection Act

5.1.2 End-User Devices

Encryption Method: Full disk encryption or file-based encryption.

Description: All personal data on end-user devices such as laptops, desktops, and mobile devices will be encrypted. This ensures that if a device is lost or stolen, the data remains inaccessible to unauthorised users.

Tools: BitLocker, File Vault, or other device-specific encryption tools.

Access Control: Strong passwords or two factor authentication to decrypt and access the data on the device.

5.1.3 Data in Transit

All data transmitted over external networks, including the internet, must be encrypted using secure protocols (e.g., Transport Layer Security (TLS), Secure Shell (SSH)).

Encryption Method: TLS or Internet Protocol Security (IPsec).

Description: Data transmitted between systems, networks, or over the internet will be encrypted to protect it from interception and unauthorised access during transmission. This includes communications like emails, file transfers, and application programme interface (API) interactions.

Protocols: HTTPS for web traffic, VPNs for secure connections, and secure email protocols like S/MIME or PGP.

Certificate Management: Digital certificates will be used to authenticate endpoints and establish secure, encrypted connections.

5.1.4 Data at Rest

All personal data, including Personally Identifiable Information (PII), financial records, and academic records, must be encrypted using strong encryption algorithms (e.g., AES-256).

20/3/2025

Encryption Method: Database encryption, file-level encryption, or whole disk encryption.

Description: All personal data stored on servers, databases, and storage devices will be encrypted to prevent unauthorised access. Encryption at rest protects data even if physical access to storage media is compromised.

Tools: Transparent Data Encryption (TDE) for databases, volume encryption tools like Linux Unified Key Setup (LUKS), or cloud provider-specific encryption services.

Key Management: Cryptographic keys used for encryption will be managed securely, with strict access controls and regular key rotation.

5.1.5 Removable Media

Encryption Method: Hardware-based encryption or software-based encryption.

Description: Data stored on removable media, such as USB drives, external hard drives, and SD cards, will be encrypted. This ensures that if the media is lost or stolen, the data remains protected.

Tools: Tools like BitLocker To Go, VeraCrypt, or hardware-encrypted USB drives.

Access Control: Encrypted media will require authentication (password, PIN, or biometric) to access the stored data.

5.1.6 Cloud Services

Encryption Method: Server-side encryption (SSE) or client-side encryption (CSE).

Description: Data stored in cloud services will be encrypted both at rest and in transit. Cloud providers will offer built-in encryption services, while client-side encryption can be employed for additional security, ensuring that data is encrypted before it leaves the user's device.

Providers: Utilise encryption services provided by cloud providers like Amason Web Services (AWS), Asure, or Google Cloud Platform (GCP).

20/3/2025

Key Management: Leverage the cloud provider's key management services (KMS) or bring-your-own-key (BYOK) options for enhanced control over encryption keys.

5.1.7 Cryptographic keys

The Information Technology personnel are responsible for prescribing the following rules regarding key management:

a) Generating random private and public cryptographic keys
b) activation and distribution of cryptographic keys
c) defining the time limit for the use of keys and their regular updating (in accordance with risk assessment)
d) archiving inactive keys which are necessary for encrypted electronic archives
e) destruction of keys

Cryptographic Keys are managed by their owners in line with the above-mentioned rules.

Cryptographic keys will be stored in secure, encrypted environments such as Hardware Security Modules (HSMs) or dedicated key management systems (KMS) with strong access controls to prevent unauthorised access. The keys will be backed up regularly in a secure location and transmitted in an encrypted method to ensure protection at all times. Only authorised personnel with proper clearance will have access to the keys. Access will be governed by multi-factor authentication and role-based access controls to minimise the risk of unauthorised changes or access.

In the event of key loss, corruption, or destruction, the following recovery process will be employed:

Backup Retrieval: The most recent encrypted backup of the key will be retrieved from the secure storage location.

20/3/2025

Restoration Process: The key will be restored using a secure and verified restoration process. The integrity of the recovered key will be checked to ensure it has not been tampered with or corrupted during the recovery process.

Incident Response: A formal incident response procedure will be followed to investigate the cause of the key loss, corruption, or destruction, and appropriate measures will be taken to prevent future occurrences.

Notification: Relevant stakeholders will be notified about the recovery process and any potential impact on operations.

5.1.8 Managing access encryption keys

Any Head of Department or Supervisor must consult with the Information Technology personnel with respect to granting access to other employees.

Detailed procedures are to be developed by the Information Technologist in consultation with the IT Consultant.

6.0 RESPONSIBILITIES

6.1 Compliance/ Monitoring/ Review

Validity and document management

The Information Technologist shall under the direction of the principal review this policy and, update the document as necessary every six months.

a) Each Head of Department is responsible for the administrative and technical measures for all new software and equipment acquired for the use of the relevant department;

b) Each Head of Department must ensure that new equipment or software introduced is the subject of a Data Protection Impact Assessment prior to the use or acquisition of such equipment or software;

20/3/2025

c) IT Personnel shall conduct DPIAs on all new software and technologies prior to approval.

d) Policies and procedures for the registration and use of new software and equipment and reporting of issues with relation to the same are to be developed by the Information Technology personnel;

e) Penetration testing and cryptographic validation testing is to be administered every two years by an entity or individual with the requisite capacity.

f) The IT personnel shall employ measures to address findings from the penetration and cryptographic validation testing and report on these developments every six (6) months, or earlier as needed, following receipt of the results of the test.

g) A shared registration system should be implemented by the Information Technologist to facilitate the logging and management of software and equipment being utilised by the NMLS

h) A training plan should be implemented to ensure that supervisors and Heads of Department will participate in training on conducting data protection impact assessments;

i) Where staff are permitted to work remotely, the Information Technologist shall discuss with the relevant staff member encryption measures and safeguards to be put in place.

j) The NMLS will provide resources necessary for the development of competence in encryption by the main users of the policy.

k) This policy will be reviewed annually or as needed to accommodate changes in technology, legal requirements, or organisational needs.

IT Department: Responsible for implementing and maintaining encryption technologies and key management.

Head of Department: Responsible for managing staff members to adhere to this policy.

Staff: Must ensure that they adhere to this policy.

20/3/2025

Students: Must follow guidelines for protecting personal data, especially when transmitting or storing it on personal devices.

6.1.1 Reporting

The Information Technologist shall report to the principal on the effectiveness of the encryption measures and employed to protect the assets of the school and makes recommendations as to the corrective and preventative actions on an annual basis.

6.1.2 Records Management

The Information Technologist is responsible for maintaining a repository of DPIAs on all new software and IT equipment being introduced to or utilised by each department of the NMLS.

7.0 ASSOCIATED DOCUMENTS

a) NMLS Data Protection Policy

b) Access Control Policy

c) User Security Awareness and Training

d) Privacy Breach Notification Procedure Manual

e) NMLS Systems/Information Encryption Log

f) NMLS Record Storage Schedule

8.0 APPROVAL

Current Document Revision #:	
Revision Date:	March 20, 2025
Procedure Owner:	Principal
Approval Authority & Date:	
Next Revision Date/Period:	
Document Revision Note:	

Revision History

Last Revision #:	
Last Revision Date:	

20|3|2025

Change Summary:	

20/3/2025

9.0 APPENDIX

Appendix I

NMLS Systems/Information Encryption Log

Name of system/type of information	*Encryption tool*	*Encryption algorithm*	*Key size*
NMLS Website	Advanced Encryption Standard (AES)	Advanced Encryption Standard (AES)	256
Tab 3 Practice Master	Advanced Encryption Standard	AES (Advanced Encryption Standard)	256-bit
Gmail	HTTPS/TLS for web access; S/MIME or PGP for email content encryption	AES	256-bit
YouTube	HTTPS/TLS (Transport Layer Security)	AES	256-bit
Rollcall	Advanced Encryption Standard (AES)	AES	256-bit
Examination and Assignment Grade Database System	Built-in Access Database Encryption	AES	256-bit
File Storage (Server)	VeraCrypt	AES	256-bit
Cloud Storage (Microsoft 365 for Education)	Built-in encryption provided by cloud storage providers	AES	256-bit
LexisNexis	HTTPS/TLS	AES	256-bit
Westlaw & TWEN	HTTPS/TLS	AES	256-bit
VLex Justis	HTTPS/TLS	AES	256-bit
U.W.I Mona Student Administration System (SAS)			
Banner Finance System	HTTPS/TLS for web access	AES	256-bit
Hein Online	HTTPS/TLS	AES	256-bit
Congressional Digest	HTTPS/TLS	AES	256-bit
Tawk.to	HTTPS/TLS	AES	256-bit
MINISIS	Database Encryption	AES	256-bit
Online Document Repository	HTTPS/TLS for data in transit; Server-side encryption for data at rest (offered by cloud services like	AES	256-bit

20/3/2025

Name of system/type of information	*Encryption tool*	*Encryption algorithm*	*Key size*
	SharePoint, Google Workspace, etc.)		
Microsoft 365	HTTPS/TLS	AES	256-bit
WhatsApp	End-to-End Encryption	Signal Protocol (AES-256 for encryption, HMAC-SHA256 for integrity, Curve25519 for key exchange)	AES-256
UWI Exchange	HTTPS/TLS	AES	256-bit
Peoplesoft	HTTPS/TLS for web access	AES	256-bit
Zoom	End-to-End Encryption (E2EE)	AES	256-bit
Google Workspace Applications (Forms, meet and docs)	Client-Side Encryption (CSE)	AES	256-bit
Turnitin	Advanced Encryption Standard (AES)	AES	256-bit

30/3/2025

Appendix II

NMLS Record Storage Schedule

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Practice Master Tabs 3	Server and Local Backup	IT Consultant/ Information Technology Personnel	Only MITS can have access to the Firewall. Only IT Consultant/ Information Technology Personnel can access server and local back-up. Access is restricted via user authentication and permissions setting	Records are stored for a period of 10 years
The Data is encrypted using SQL database to ensure confidentiality, with access limited to authorised users with decryption keys.	Company Intranet	IT Consultant/ Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish the instructions	Instructions that are no longer valid are stored for a period of 3 years
The rules for the encryption key management are stored in a designated folder on the company intranet, accessible only to	Company Intranet	IT Consultant/ Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish the rules	Rules that are no longer valid are stored for a period of 3 years

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
authorised personnel				
Roll Call	AWS	IT Consultant/ Information Technology Personnel	Only Authorised users have access rights to such records	Instructions that are no longer valid are stored for a period of 10 years
The Data is encrypted using SQL database to ensure confidentiality, with access limited to authorised users with decryption keys.	Company Intranet	IT Consultant/ Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish the instructions	Instructions that are no longer valid are stored for a period of 3 years
The rules for the encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/ Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish the rules	Rules that are no longer valid are stored for a period of 3 years
File Storage	Server and Local Backup	IT Consultant/ Information Technology Personnel	Only Authorised users have access rights to such records	Rules that are no longer valid are stored for a period of 10 years
The Data is encrypted using SQL database to	Company Intranet	IT Consultant/ Information Technology Personnel	Only Information Technology	Instructions that are no longer valid

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
ensure confidentiality, with access limited to authorised users with decryption keys.			Personnel has the right to edit and publish the instructions	are stored for a period of 3 years
The rules for the encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/ Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish the rules	Rules that are no longer valid are stored for a period of 3 years
PaperCut (Print Management Software	Company Intranet	IT Consultant/ Information Technology Personnel	Only Authorised users have access rights to such records	Rules that are no longer valid are stored for a period of 10 years
The Data is encrypted using SQL database to ensure confidentiality, with access limited to authorised users with decryption keys.	Company Intranet	IT Consultant/ Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish the instructions	Instructions that are no longer valid are stored for a period of 3 years
The rules for the encryption key management are stored in a	Company Intranet	IT Consultant/ Information Technology Personnel	Only Information Technology Personnel has	Rules that are no longer valid are stored

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
designated folder on the company intranet, accessible only to authorised personnel			the right to edit and publish the rules	for a period of 3 years
NMLS Website	AWS	IT Consultant/Information Technology Personnel	Only authorised users have access rights.	Instructions that are no longer valid are stored for a period of 10 years.
Data is encrypted using AES with 256-bit key.	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions.	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel.	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules.	Rules that are no longer valid are stored for a period of 3 years.
Gmail	Google Cloud	IT Consultant/Information Technology Personnel	HTTPS/TLS for web access; S/MIME or PGP for email content encryption.	Instructions that are no longer valid are stored for a period of 10 years

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data is encrypted using AES with 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions.	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel.	Company Intranet	IT Consultant/Information Technology Personnel	The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel.	Rules that are no longer valid are stored for a period of 3 years.
<u>YouTube</u>	Google Cloud	IT Consultant/Information Technology Personnel	HTTPS/TLS for web access	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions.	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has	Rules that are no longer valid are stored

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
designated folder on the company intranet, accessible only to authorised personnel.			the right to edit and publish rules.	for a period of 3 years.
Examination and Assignment Grade Database System	Server and Local Backup	IT Consultant/Information Technology Personnel	Only authorised users have access rights.	Instructions that are no longer valid are stored for a period of 10 years
Database encryption with AES using 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions.	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel.	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules.	Rules that are no longer valid are stored for a period of 3 years.
Cloud Storage	Cloud provider (AWS, Azure,	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
	Google Cloud)			for a period of 10 years
Data is encrypted using AES with 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel.	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years
LexisNexis	Cloud provider (AWS)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has	Rules that are no longer valid are stored

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
on the company intranet, accessible only to authorised personnel			the right to edit and publish rules	for a period of 3 years.
Westlaw & TWEN	Cloud provider (AWS)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
VLex Justis	Cloud provider (AWS)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
<u>Banner</u>	UWI Intranet	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet,	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
accessible only to authorised personnel				
<u>Hein Online</u>	Cloud provider (AWS)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
<u>Congressional Digest</u>	Cloud provider (AWS)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit	Instructions that are no longer valid are stored

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
			and publish instructions	for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
Tawk.to	Cloud provider (AWS)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
MINISIS	Cloud provider (AWS)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
Online Document Repository	Cloud provider (AWS or other cloud provider)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years.
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
Microsoft 365	Cloud provider (Microsoft Azure)	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
WhatsApp	Cloud provider (AWS or	IT Consultant/Information Technology Personnel	End-to-End Encryption with Signal Protocol	Instructions that are no longer valid are stored

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
	other cloud provider)			for a period of 10 years
Data is encrypted using AES-256 for encryption, HMAC-SHA256 for integrity, and Curve25519 for key exchange	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
UWI Exchange	UWI Intranet	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has	Rules that are no longer valid are stored

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
on the company intranet, accessible only to authorised personnel			the right to edit and publish rules	for a period of 3 years.
<u>Peoplesoft</u>	UWI Intranet	IT Consultant/Information Technology Personnel	Server-side encryption (SSE) or client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
<u>Zoom</u>	Cloud provider (AWS or other cloud provider)	IT Consultant/Information Technology Personnel	server-side encryption (SSE) and client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology	Instructions that are no longer valid

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
			Personnel has the right to edit and publish instructions	are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.
Google Workspace Applications (Forms, meet and docs)	Google's own cloud infrastructure.	IT Consultant/Information Technology Personnel	server-side encryption (SSE) and client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.

20/3/2025

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Turnitin	Cloud provider (AWS or other cloud provider)	IT Consultant/Information Technology Personnel	server-side encryption (SSE) and client-side encryption (CSE)	Instructions that are no longer valid are stored for a period of 10 years
Data is encrypted using AES with a 256-bit key	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish instructions	Instructions that are no longer valid are stored for a period of 3 years.
The rules for encryption key management are stored in a designated folder on the company intranet, accessible only to authorised personnel	Company Intranet	IT Consultant/Information Technology Personnel	Only Information Technology Personnel has the right to edit and publish rules	Rules that are no longer valid are stored for a period of 3 years.

AS 20/3/2025

References

[i] Project Management Institute. (2013). A guide to the project management body of knowledge (PMBOK®guide) – Fifth edition. Newtown Square, PA: Author.

[ii] https://www.ibm.com/topics/cryptography

[iii] https://nordvpn.com/cybersecurity/glossary/cryptographic-key/

[iv] https://www.ibm.com/topics/encryption

[v] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

[vi] Definition from Search Security

[vii] Techcopedia.com

[viii] https://nordvpn.com/cybersecurity/glossary/decryption/

20/3/2025