ONEUNIVERSE INFORMATION SECURITY POLICY

July 2025

Document Control Sheet

Document Title	ONEUNIVERSE – Information Security Policy V1.0
Type	Information Security Management System
Document Author	Chief Information Security Officer
Document Owner	Information Security Office
Date	July 2025
Managed by	Information Security Office
Next Review Date	July 2027
Document Classification	Confidential /All Employees

Document History – Change Record

Issue Date	Issue No	Obsolete/Current/Archived	Reason/Notes
25/07/2025	Issue 1	Current	

Reviewers and Approvals

This document has been reviewed and approved by:

Name	Position	Signature	Date
	Managing Director (MD)		
	Head Business Technology		
	Chief Information Security Officer (CISO)		

INTRODUCTION

Information must be protected in a manner commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored (paper, electronic media, computer bits, etc.), the systems, which process it (computers, mainframes, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.). Such protection includes restricting access to information based on the need-to-know principle.

This policy is governed by the **OneUniverse Information Technology Governance Framework** that supports Enterprise Risk Management and is a management tool to ensure business success.

OBJECTIVE

There are 3 security control objectives that address the Information Security requirements, which are as follows:

Confidentiality	The restriction of data to those authorised to see it.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Availability	The property of being accessible and usable upon demand by an authorised entity.

SCOPE

This policy applies to all employees of OneUniverse, as well as contractors and third parties and their employees. This policy is also applicable to people, processes and technology that manage OneUniverse information systems and data resources including 4IR technology, cloud based and hosted infrastructure, systems, data and applications.

End Users must comply with this policy as well as the related policies, standards and guidelines when interacting with OneUniverse information resources to maintain confidentiality, integrity and ensure appropriate availability.

COMPLIANCE

All instances of non-compliance with this standard, whether intentional or not, must be identified by the Business Entity. Non-compliance with this standard may result in disciplinary action being taken in terms of the disciplinary codes and procedures, up to and including termination of service and legal or criminal proceedings being taken. Deviations from the minimum requirements of this standard must be approved through the Managing Director.

ROLES AND RESPONSIBILITIES

General information

Information Security vs Cyber Security

When using this policy, it is important to understand the difference between information security and cyber security:

Information security is the broad practice of protecting and preserving the integrity, confidentiality and availability of information assets and information technology. The scope of information security includes both digital and physical formats of information.

Cyber security is more specific and narrower in scope. The word "cyber" generally relates to computer systems and the internet. Cyber security refers to protecting, securing and preserving digital information, internet facing and interconnected systems from threats.

CULTURE AND AWARENESS

Information Security Training

- To ensure a deep compliance culture, the following shall be considered:

Adherence to regulatory standards	Information Security awareness, education and training	All Board Members and employees of OneUniverse and, where relevant, contractors shall receive appropriate awareness education and training (At least once a year) in relation to information security.

Accepted Information Security Practices

- **NIST CYBER SECURITY FRAMEWORK** under the function “Protect” – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- A critical part of the Protect function also involves supporting efforts with security education. Under this category, security decision-makers must train personnel so that they can efficiently and effectively carry out the protection tasks outlined in the company’s policies and vendor agreements.
- **COBIT 5** Training and education support external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture, and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.
- **ITIL** also refers to the development of an ISMS, which in turn speaks to training requirements.
- **King IV Principle 12** requires that a governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives. Principle 13 further requires that a governing body should govern compliance with applicable laws and adopted, non-binding rules, codes and standards in a way that supports the organisation being an ethical and good corporate citizen. This implicitly requires that an Information Security Management System appropriate to the business must be established and maintained. (Refer to 1 above) From a risk perspective, this ensures that we

are aligned with this principle of being a good corporate citizen. Not only does the training benefit them as individuals, but also as individuals who access our IT systems and deal with OneUniverse owned data.

- There is **no cost** involved to the contingent workers completing this training. There is also no cost to their employer.
- **Contractual obligations:**
- OneUniverse contracts contain the following clauses: *When providing the Services, the Vendor will adhere to:* ***OneUniverse policies, code of conduct, rules, procedures and regulations****, including specifically security regulations and access to One Universe's information resources, networks and systems, in force and as amended from time to time, which are available on request or may be accessed (Please insert link to OneUniverse Website). Where OneUniverse grants the Vendor permission to remotely access its infrastructure and or network, the Vendor will adhere to OneUniverse policy relating to remote access, provided that unless otherwise expressly stated by the OneUniverse in writing, the Vendor will have "read only" access to its infrastructure and/or network.*

- **Consequences for not completing mandatory training:** In addition to the consequences listed under "Section 4 – Compliance" of this policy, the OneUniverse Chief Information Security Officer (at discretion) has the right to remove enterprise access entitlements for any user who does not complete their mandatory Information Security Training within the enforced timeline, until such time that the training has been completed.

Cultural Behaviour

For any person identified by the Cyber Security Office, through its processes, to be displaying irresponsible information and cyber security behaviour that unnecessarily places OneUniverse at risk, the Chief Information Security Officer (at discretion) has the right to revoke enterprise access for that person, pending possible disciplinary and or remedial training outcomes.

INFORMATION SECURITY OPERATIONS

Asset Management

Information and other assets associated with information and information processing facilities must be identified and an inventory of these assets must be drawn up and maintained.

Assets maintained in the inventory must have an assigned owner.
All end users in possession of OneUniverse owned assets are responsible for ensuring that these assets are well maintained and the information within them is kept secure at all times.

An appropriate set of procedures for information labelling and procedures for handling OneUniverse assets shall be developed and implemented by OneUniverse.

HR SECURITY

All employee responsibilities and duties must be terminated immediately after employment termination.

Any information security responsibilities and duties that remain after employment termination or change of employment must be defined and communicated to the respective employee, contractor and third party.

OPERATIONS SECURITY

Refer to the following points below:

Malicious Code

Detection, prevention, response and recovery controls to protect against malware must be implemented within the OneUniverse *e* environment, combined with appropriate user awareness.

Any device used for business purposes, whether or not company owned, that is known to be vulnerable to computer malicious code (e.g., virus) attack, must be protected by OneUniverse approved anti-malware measures.

It is prohibited to intentionally write, generate, compile, copy, propagate, execute, transmit or attempt to introduce any computer code designed to self-replicate, damage, unlawfully record, or otherwise degrade the performance of OneUniverse information resource.

Users must not attempt, under any circumstances, to eradicate viruses from their systems. If users suspect infection by a computer virus or malware, they must immediately stop using the information system and call the IT helpdesk.

Hyperlinks and/or QR Codes

Non system generated hyperlinks in all non-secure communication mechanisms considered to be untrusted (e.g., email, messaging, social platforms, etc), that are widely used and targeted by malicious actors to distribute malicious content, must be avoided where possible.
Instead trusted, secure mechanisms and platforms must be used as per OneUniverse strategy. Where it is unavoidable or a sound business case prevails, such instances must be approved by the Chief Information Security Officer and the Managing Director.

Information Backups

Information must be backed-up in a secure and reliable manner to ensure that business operation is not impaired in the event of information loss.

Backups must be performed in accordance with a defined back-up retention cycle that reflects business needs and considers the criticality of the information. The frequency of backups must support a recovery time to limit business impact to an acceptable level.

Backup procedures must be documented in an approved manner.

Regular restore testing must be done to ensure recovery and retrieval is possible in the event of data loss. Tests must evaluate if data confidentiality and integrity is maintained during recovery or retrieval and that it may be done within an acceptable timescale (i.e., the point beyond which unacceptable loss would be suffered).

Onsite and offsite restore procedures must be in place to support the restore and recovery objectives of the overall business continuity or disaster recovery plan.

OneUniverse information stored locally on user computers and share drives must be backed-up on a regular basis to its dedicated network. The responsibility for this process lies with the End User.

Monitoring

Information security status information must be gathered to enable compliance measurement against OneUniverse policy and standards, best practice, legal and statutory requirements.

Management reports must be provided for review to indicate progress toward identified goals.

Risk managers, Information Owners, System Owners and ISO's must measure the effectiveness of security controls through ongoing monitoring of the impact of information security incidents against benchmarks. Deviations must evoke analysis and corrective action.

Monitoring significant changes in the exposure of information to major threats must be done on a continual basis for all information.

Change Management

All changes to information resources e.g., systems must be applied in a secure, managed and reliable manner to ensure minimum impact to business operation. Formal change management must incorporate information processing and information resource e.g., system changes of any kind that could potentially impact business operation.

The change management process must be separate from the development and operational processes.
Changes must be requested through a formal documented change request. The change request must include the following information for approval by all affected parties:

- Changes must be traceable, and documentation updated.
- Documentation describing the proposed changes must be maintained and adequate audit trails provided to track the steps followed in implementing the changes.

Emergencies arise which require action to be taken to limit the impact to current operations in a timeframe that does not allow time for a formal change control procedure. Procedures must be in place for emergency changes to be logged on the change request system even if it is after the event.

Access Control

Access to OneUniverse information and resources must be restricted to those entities that have a legitimate business need and have been specifically authorized or granted through an approval process in accordance to the “Least Privilege” principle. Individual accountability (non-repudiation) must be assured at all times.

The Information Owners/System Owners must ensure that all system access privileges are removed as soon as they are made aware that the employee no longer needs the access.

The Information Owners/System Owners must ensure that system access privileges are suspended when employees proceed on annual leave. Business Entities may limit the system access that is restricted based on the individual business’ requirements. The user is responsible for requesting re-instatement of this access on their return from leave.

Distribution of passwords must be done in a secure manner and to the intended user only.

Access must comply with legal, regulatory, statutory and contractual obligations. The computer and communications system privileges of all users, systems, and independently operating programs (such as “agents”) must be restricted based on the need-to-know. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.
A formal process of re-certification/attestation to verify access rights given to end user within information processing resources must be completed at least bi-annually.

Business Continuity

The security aspects of the business requirements, system design, and system build, or acquisition must conform to the security architecture and Information System standards.

Computer Operations management must establish and use a logical framework for segmenting information resources by recovery priority. This will in turn allow the most critical information resources to be recovered first.

Management must prepare, periodically update, and regularly test a disaster recovery plan that will allow all critical computer and communication systems to be available in the event of a natural disaster.

Information assets must be retained and stored in accordance with the accepted retention and destruction procedures.

Vendor Relationships

Outsourcing

OneUniverse security requirements must be addressed when outsourcing any element of an information resource including a system or any information storage, transmission or processing or support function.

OneUniverse must subject the selection of outsource service providers to a formal process prior to outsourcing and must comply with approved Vendor risk management framework.

All relevant processes including legal and OneUniverse Procurement requirements for outsourcing agreements and arrangements must be complied with.

Third Party Management

All third-party Vendor s must comply with the relevant OneUniverse policies and standards.

Information security requirements for mitigating the risks associated with Vendor's access to the OneUniverse assets will be agreed with the Vendor and documented.

All relevant information security requirements shall be established and agreed with each Vendor that will access, process, store, communicate or provide infrastructure components to the OneUniverse.

Line/Business Management must monitor and review Vendor service delivery at least annually.

Cryptography

OneUniverse information, where required must be encrypted in line with approved Cryptography Functional Standard/Policy.

Whenever encryption is used, end users must not delete the sole readable version of the information unless they have first demonstrated that the decryption process is able to re-establish a readable version of the information.

If encryption keys / certificates are used for system-to-system encryption these keys must be utilised and stored in accordance with OneUniverse Cryptography Functional Standard.

Encryption keys used for OneUniverse information must always be classified as "Restricted" information. Access to such keys must be strictly limited to those who have a need-to-know. Approval from the relevant appropriate ISO and Chief Information Security Officer (CISO) is required prior to encryption keys may be shared with consultants, contractors or third parties. Encryption keys must always be encrypted when sent over a network.

Mobile and Teleworking Security

Users must ensure that storage and transportation of OneUniverse information on removable media devices is done in a secure manner.

When removable media devices are used for backups, such backups must be with the consent of the Information Owner and the retention of data must comply with the OneUniverse retention requirements.

When disposing of information storage media containing “Confidential” or “Restricted”, this must be done in line with approved requirement.

OneUniverse prohibits the use of mobile devices in high-risk facilities containing information processing resources, storing, or transmitting classified information unless specifically permitted by the Risk Manager and Information Owner of that area. The OneUniverse reserves the right to enforce restrictions on individuals permitted to use mobile devices in facilities containing information processing resources.

The OneUniverse enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information processing facilities, storing, or transmitting classified information.

- Connection of managed devices to classified information systems must be approved by the system and information owner. The information stored on those devices are subject to random reviews/inspections by defined security officials, and if classified information is found, the incident handling policy is followed.

Use of internal or external modems and wireless interfaces simultaneously within the mobile devices is prohibited while there is a connection to the OneUniverse ’s internal network.

Information Security Incident Management

All incidents that impact business operations must be managed to minimise any adverse impact, thus ensuring that the best possible levels of service quality, confidentiality, integrity and availability are maintained.

Roles and Responsibilities

The roles and responsibilities for addressing incidents must be defined and assigned, including formal incident management and emergency response processes. All End Users must report incident(s) as soon as they recognise that an incident has occurred on a timely basis so that prompt remedial action can be implemented.

Management must ensure that there are appropriate measures and plans in place to combat cyber threats in a timely manner and to protect the confidentiality, integrity and availability of all critical and non-critical information systems.

Detection and Recording

All reported and detected incidents must be recorded in a standard and consistent manner so that they can be tracked, monitored, and updated throughout their life cycle.

Incidents must be categorised, prioritised and assigned so they can be handled as effectively as possible to determine subsequent appropriate action to be taken for timely resolution.

All recorded incidents must be investigated and analysed to determine the underlying causes, appropriate and timely recovery and resolution.

Incidents must be escalated when necessary to ensure that identified incidents are resolved in the most efficient way and on a timely basis.

Recorded incidents must be appropriately handled and responded to efficiently and timely. The classifications and analysis/diagnosis results must determine the way the response and handling of incidents is to be managed.

All incidents must be reported to determine the status of reported "Incidents not resolved" and in assisting with trend identification. These reports must be adequately analysed and acted upon.

Testing and Recovery

Management must prepare, periodically backup and update, and regularly test emergency response plans. These plans must provide for the continued operation of critical systems in the event of an interruption or degradation of service.

COMMUNICATION SECURITY

Domain Registration

All domain name system, information management, registration, migration and hosting services shall be implemented via a centralised process to ensure that the OneUniverse trademarks are adequately protected.

All fully qualified domain names in use for email communications to customers or websites serving web pages to customers, must be owned and managed by the OneUniverse. All security measures such as cloning, phishing or copyright monitoring must be applied.

Naming Conventions

All devices must be named in accordance with the OneUniverse naming convention standard in order that the relevant business unit responsible for the device can be identified.

Network Security

Network custodians must implement measures to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of any information travelling over OneUniverse computer networks.

All network devices must display a OneUniverse approved banner advising End Users of the OneUniverse policies.

Managed vs Self-managed Devices

All managed devices connecting to the OneUniverse 's network must comply with the required baseline standard.
Baseline controls and standards have been defined for selected technologies to implement current good practice for each technology. Compliance with these standards is mandatory.

In the absence of a OneUniverse baseline for a specific technology, common best practice must be applied to secure devices.

In the event that a non-compliant device is discovered, and/or is assessed as being seriously vulnerable, the Network Custodian shall disconnect the device in line with defined process.

Network Perimeters

All network perimeters must be compliant to applicable policy instituted by OneUniverse.

Access control mechanisms on any network device must support applying “Least Privilege” to all entities and devices.

Security reviews must be conducted at least annually or when major changes have been made to critical bank infrastructure to assess the adequacy of network management, traffic management, network operations and security management.

Business risks associated with the network must be assessed by evaluating the network's vulnerability to key threats in conjunction with reviewing the information security requirements of the business applications supported by the network.

Technically proficient persons in the Internal Audit department, Risk Management area or working for an authorized third party must perform assessment to provide objective assurance on the status of security. Those responsible for either the administration or management of the involved network devices must not perform reviews.

External Connectivity

No device may be connected to an external or untrusted network (e.g., via modem, Wi-Fi, switch) and the internal or trusted network simultaneously without the written approval of the Chief Information Security Officer and must be audited to ensure that it is protected in line with applicable standard set by OneUniverse.

Demilitarized Zone

A demilitarized zone (DMZ) must be implemented using approved firewalls where servers, accessed from networks not managed by entities within the OneUniverse are placed.

Services/applications placed in the DMZ, may initiate connections through the firewall to the internal network only if host-to-host connectivity is allowed; and if the conditions set out by the network perimeter custodians are met.

Network Intrusion Detection Systems

Network Intrusion Detection Systems (NIDS) must be connected to the network so that they can monitor traffic from all relevant perimeter access points. NIDS must also be able to monitor outbound traffic to the Internet from the internal network on the inside of the firewall.

A filter for commonly used protocols must be implemented for outbound browsing.

Remote Access Services

Remote access to the OneUniverse network and resources is available to OneUniverse employees and Third Parties on approval by Management, Information Security Officials and Information Owners, and in accordance with the OneUniverse standard governing remote access.

Traffic must be encrypted (from the point of connection on the non-OneUniverse network, to the termination point within the OneUniverse network) and the End User must not be able to break out of the encrypted session such as through split tunnelling. During this session, the remote computer must be protected from connections by other hosts on the non-OneUniverse network.

System Event Logging

All systems must retain event logging that enables the ability to identify End User access and the +reconstruction of transactions performed.

All events logged must be retained in a location and format where log retrieval is possible and tampering or deletion of log is not possible.

Access to view logs must be limited to appropriately authorised individuals.

Vulnerability Management

Information about technical vulnerabilities of information systems being used must be obtained in a timely fashion.

OneUniverse exposure to identified vulnerabilities must be evaluated and appropriate measures must be taken to address the associated risk (e.g., by performing regular vulnerability assessments and penetration tests).

Continuous discovery, remediation and monitoring of vulnerabilities must be carried out regularly to prevent information systems from being exploited.

Physical Security

All OneUniverse equipment must be physically secured. OneUniverse network, servers and communication equipment must be stored in a secure, access and climate-controlled Data Centre, in specially designated racks. Access to the Data Centre must be restricted and reviewed on a regular basis.

Computer equipment must be physically protected to lessen the risks of theft, destruction, and/or misuse. Controls to reduce these risks include housing the equipment in a locked room, physically locking the equipment to its workstation desk, or providing guard service or other physical security to protect the premises containing computers.

Each piece of computer equipment must be marked for identification and inventory control. Inventory records of computer equipment must be kept up to date.

Computer equipment (except for mobile devices) must not be moved or relocated without the prior approval of the responsible business unit head, system owner or another approved delegated person.

Employees who must not remove “Restricted or Confidential” OneUniverse information from OneUniverse offices. In cases where “Restricted or Confidential” OneUniverse information needs to be removed for work purposes or printed at home; a risk assessment form needs to be completed together with the employee’s ISO. Reasonable and appropriate measures must be taken to ensure that the information is kept secure. All OneUniverse information must be returned immediately on resignation or termination of employment.

“Restricted” information must not be downloaded to remote locations unless proper physical security and encryption facilities are installed and faithfully observed.

Acquisition, Development and Maintenance Security

Management shall ensure that development, testing and operational environments are separated to reduce the risk of unauthorised access or changes to the operational environment. Accountability for changes made to all environments must be maintained.

Responsibility for compliance with OneUniverse policies and frameworks, best practice, regulatory and statutory requirements must be designated as part of the information system development and acquisition processes.

Systems development and acquisition activities must be carried out in accordance with a formal approved methodology (SDLC). The methodology must include methods for documenting and ensuring that information security requirements are met. Compliance with the methodology used must be monitored.

Quality assurance activities must include a formal assessment of risks. Such risks must be assessed at an early stage of the process, documented, and reviewed at key stages during the development/implementation lifecycle. Action must be taken to minimise risks by considering alternative approaches, revising staffing arrangements or plans and cancelling activities with unacceptable risks.

Prior to introduction of new information system development changes, a formal approved test procedure must be performed. Where there is a requirement for testing to be done using “live” or production data, this must be requested, assessed, and approved by the System Owner, Business CIO and ISO.

Deployment into the live production environment must be done in accordance with the Change Management Policy and Guidelines.

DOCUMENT RULES AND ADMINISTRATION

Copyright and Confidentiality

No part of this document may be reproduced, transferred, sold, or otherwise disposed of, without the written permission of OneUniverse. This document can be used and copied within OneUniverse only. However, no copies can be forwarded to any person who is not an employee or agent of OneUniverse without the prior written approval of OneUniverse.

Authoritative Source

This document, once downloaded from the document management system, is an uncontrolled copy, which is no longer guaranteed to be authoritative.

Document Changes

Please advise the author of any concerns or discrepancies relating to this document such as:

- Errors
- Omissions
- Ambiguities
- Requests for change
- Suggestions for improvement

References

This policy must be read in conjunction with other applicable frameworks, policies, and standards:

ABBREVIATIONS AND DEFINITIONS

Definitions of terms used in this document.

Abbreviation/Definition	Description
Access	The ability to use, modify or manipulate an information resource or to gain entry to a physical area or location.
Availability	Protection of IT systems and data to ensure timely and reliable access to and use of information to authorised users.
Compliance	Conforming to a rule, such as a specification, policy, standard or law.
Cyber Security Incident	Any cyber related act or attempted act perpetuated by organised crime syndicates, hacktivist OneUniverse s or any other external individual or OneUniverse of people with malicious intent, that have the capability to perform a significant criminal act against OneUniverse or any of their stakeholders.
Data	Information that is recorded in any format, whether stored electronically or in a paper-based form. Note: For the purpose of this policy, Data implies Information and Information implies Data hence the two can be used interchangeably to denote the same intention.
Devices	A device is a unit of hardware, outside or inside the case or housing for the essential computer (processor, memory, and data paths) that is capable of providing input to the essential computer or of receiving output or of both. These devices include personal devices, where end users are permitted to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.
DMZ	Demilitarized Zone – Secure isolated area of the network.
Email filter	Content filter checking for Malicious Code, size, type of files etc.
End user	Including: • Permanent employee. • Contractors, temporary staff. • Third parties and/or business partners.
OneUniverse	OneUniverse which includes all affiliates, subsidiaries, franchises and segments
Information	The data processed, captured, stored and/or transmitted on the OneUniverse 's information systems regardless of the media used
Information Asset	Computers, communications facilities, networks, data (information) and encryption keys that may store, process, retrieve or transmit information. This includes programs, specifications, and procedures for their operation, use and maintenance. All such assets are the property of OneUniverse and must be protected per OneUniverse policies.
Information Owner	The information owner is an individual who is responsible for the information with the system.

Abbreviation/Definition	Description
Information Security	Information security is the provision of organisational, technical, and social measures to safeguard information assets against unauthorised access, damage and interference - both malicious and accidental.
CISO ISO	Chief Information Security Officer. Information Security Officer.
Malware	Malicious software, such as a virus or unauthorised program, which is specifically designed to disrupt or damage a computer system.
May	This word or the adjective "Optional" means that a policy statement is optional.
Must	This word, or the terms "Required" or "Shall", mean that the definition is an absolute requirement of the policy.
NIDS	Network Intrusion Detection System.
Policy	A policy is a set of rules and principles that must be adhered to and is approved. The purpose of a policy is to establish accountability, roles and responsibilities, to direct management and formalise the requirements and standards for implementing measures in a consistent and cost-effective manner.
Security Incident	A security incident is defined as any breach of the requirements of ONEUNIVERSE information security policies.
Segregation of Duties (SOD)	A control that is designed to ensure that one individual is never responsible for completing or controlling a task from beginning to end to prevent fraud or abuse.
Self-Managed Devices	Servers not managed by FNB I&SS but rather managed by the respective BU.
SDLC	Software Development Lifecycle
Shall	This word, or the terms "Required" or "Must", mean that the definition is an absolute requirement of the policy.
System owner	The system owner is an individual who is accountable for the system and its applications.

DOCUMENT CONTROL

Document Restrictions

This document contains information that is intended for consumption within OneUniverse and as a result it is classified as “Confidential”. The purpose of the document is to record and communicate OneUniverse Information Security Policy to authorised stakeholders.

Distribution of this report to any unauthorised external party is strictly prohibited. This document must be handled in accordance with the prescripts of the information classification standard as it pertains to information classified as “Confidential”.

In the event that this document must be distributed to and shared with external entities, a formal request must be submitted to the document owner, as specified in the Document Control section.

Document Audience

Anyone involved in the management, configuration, administration, maintenance, support, or use of Information Security, as well as those who have responsibilities for or are otherwise interested in the subject.

Note:

This policy is relevant at a OneUniverse level which includes all subsidiaries and segments within its structures.