IT Security Audit Types

Security Audit	Time of Essence Audit
Description	A Time of Essence Audit is a security audit, which has to be undertaken immediately because of its potential critical impact on the University's infrastructure or legal obligations.
Purpose	• Ensure the continuing operational integrity of the University's infrastructure. • Eliminate any immediate adverse impact on external sites or organisations originating from within the University's IT infrastructure. • Comply with legal or police requirements of an urgent, time critical matter.
Inclusions/ Exclusions	Actions carried out under this type of audit will be limited to minimal material or information required to satisfy requirements set out above and record for University audit purposes.
Authority	This audit is undertaken by the IT Security Team or delegated officer.

Security Audit	Proactive Integrity Audit
Description	A Proactive Integrity audit is a security audit to proactively identify security risks to the University's IT and communications infrastructure.
Purpose	This audit is undertaken to proactively protect the University's IT and Communications infrastructure.
Inclusions/ Exclusions	This audit will attempt to identify risks and vulnerabilities of services and equipment connected to the University communication facilities through: • Random probes of connected equipment for vulnerabilities • Scanning of the network for known security threats, such as viruses • Scanning of the network for hardware, software or services that would violate commercial agreements (e.g. unlicensed software), laws (e.g. copyright material, images) or University regulatory compliance requirements This audit will explicitly not include the collection of any personal or confidential information.
Authority	This audit is undertaken by the IT Security Team or delegated officer.

Security Audit	Investigative Audit
Description	An Investigative Audit is a security audit where a significant amount of confidential material is collected over a period of time.
Purpose	An Investigative Audit brief will be prepared for signoff by the Pro Vice-Chancellor and Chief Information Officer or delegates. This brief will contain the following information: • The reason for requesting the audit • The scope of the audit investigation • The specific outcomes or deliverables of the audit • The proposed duration of the audit • Who will be involved in the audit • The University facilities that will be involved/investigated/interrogated in performing the audit At the end of the Investigative Audit a report will be created to document the following information: • The date that the final investigation was completed • All paper printouts that were assembled as part of the investigation • A listing of all electronic files created electronically during the investigation • If necessary a statement confirming all electronic files were deleted at the end of the investigation • A copy of the audit findings
Inclusions/ Exclusions	The collection of confidential material over a period of time as defined in the Investigative Audit brief.
Authority	This audit is undertaken by the IT Security Team or delegated officer and requires sign-off by the Pro Vice-Chancellor and Chief Information Officer or delegates.

Security Audit	Information Collation Audit
Description	An Information Collation Audit is an audit of any type of storage medium (hard disk drives, portable storage etc.) with the aim to identify and recover vital corporate information. An example is when an employee leaves the University but fails to pass on vital information collected or created during the course of his/her employment.
Purpose	• This type of audit must be authorised by an appropriate senior manager and any information gathered returned to that senior manager • Each request should also be approved by the Pro Vice-Chancellor and Chief Information Officer and the Manager IS Service Quality • All requests for such audits must be logged through the Service Desk so they are properly recorded and can be referenced at a later date, but no identifying information is to be recorded in the log
Inclusions/ Exclusions	Recovery of vital corporate information.
Authority	This audit is conducted at the request of a senior manager for the organisational use of that senior manager

Security Audit	Telephony Audit
Description	A security audit of the University's telephony infrastructure to investigate non-appropriate use.
Purpose	• This type of audit must be authorised by an appropriate senior manager and any information gathered returned to that senior manager • Each request should also be approved by the Pro Vice-Chancellor and Chief Information Officer and the Manager IS Service Quality • All requests for such audits must be logged through the Service Desk so they are properly recorded and can be referenced at a later date, but no identifying information is to be recorded in the log
Inclusions/ Exclusions	This audit includes the identification of risk and/or vulnerabilities based on a non-appropriate use of the University's Telephony infrastructure by students, staff or external users or a non-appropriate configuration of the system. The Telephony Audit shall include the following security checks: • Unauthorised use of telephony resources i.e.: An extension might incur a substantial cost because of an unauthorized use of the telephony system. The audition process will include an analysis of the "Call Detail Records" (CDR) that are stored in the Telephony System. • Suspicious/Malicious calls: If a student, staff or external user receives a call into the University telephony system from a suspicious source it may be considered a security risk or threat through the Telephony system. The audition process will include the validation of usage of the "Malicious Call Trace" (MCT) feature into any University Telephony Platform. • External transferred conference: External "Trunk to Trunk" connectivity shall be disabled in every Telephony Platform for avoiding 3rd party to 3rd party (only) transferred conferences. • Privacy Intrusion through "Intrusion" feature configured to a non-appropriate user. ("Intrusion" feature allows a user to intrude on an active call). • Privacy Intrusion through "Barge In" feature configured to a non- appropriate user. ("Barge In" feature allows an user to join into an active conference without being invited by any conference member) • Privacy Intrusion through "Conference Tone" during a multiparty voice conference. (If the "Conference Tone" is disabled in the Telephony Platform, conference members will not sense if there is more than one (1) participant in the call).
Authority	This audit is conducted at the request of a senior manager for the organisational use of that senior manager