Smartcall IT Security Policy

The Smartcall IT Security Plan defines the information security standards and procedures for ensuring the confidentiality, integrity, and availability of all information systems and resources under the control of Smartcall Information Technology

Disclaimer

DISCLAIMER OF WARRANTY - THE INFORMATION CONTAINED HEREIN IS PROVIDED "AS IS." SMARTPHONE SP (PTY) LTD T/A SMARTCALL MAKES NO EXPRESS OR IMPLIED WARRANTIES RELATING TO ITS ACCURACY OR COMPLETENESS. SMARTPHONE SP (PTY) LTD T/A SMARTCALL SPECIFICALLY DISCLAIM ALL WARRANTIES, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SMARTPHONE SP (PTY) LTD T/A SMARTCALL BE LIABLE FOR DAMAGES, INCLUDING, BUT NOT LIMITED TO, ACTUAL, SPECIAL, INCIDENTAL, DIRECT, INDIRECT, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL, COSTS OR EXPENSES (INCLUDING ATTORNEY'S FEES WHETHER SUIT IS INSTITUTED OR NOT) ARISING OUT OF THE USE OR INTERPRETATION OF SMARTPHONE SP (PTY) LTD T/A SMARTCALL POLICIES OR THE INFORMATION OR MATERIALS CONTAINED HEREIN.

Definitions

Acquisition	In the context of this document, gaining possession, through purchase or lease, of assets and/or services related to information technology, such as computer hardware, software, or services.
Accreditation	In information system security, the formal authorization for system operation and an explicit acceptance of risk given by the accrediting (management) official. It is usually supported by a review of the system, including its management, operational, and technical controls.
Audit	In IT, an independent, unbiased examination of an information system to verify that it is in compliance with its own rules; the process of collecting and evaluating evidence of an organization's security practices and operations in order to ensure that an information system safeguards the organization's assets, maintains data integrity, and is operating effectively and efficiently to meet the organization's objectives.
Auditable event	A single action (either a command or system call) that affects the security of an information system.
Backup	The process of backing up (copying onto electronic storage media) data that may then be used to restore the data to its original form after the occurrence of a data loss event or data file corruption. Two backup types are referenced in this document • Full – a complete backup of all data, whether or not changes have occurred • Incremental – a backup of only those files that have changed or been added since the last full or incremental backup was performed
Corrective Maintenance	A form of system maintenance performed after a problem or failure is detected in an information system, with the goal of restoring operability or peak performance to the system.
Criticality	Degree of value
Data Corruption	The result of errors in computer data that occur during electronic writing, reading, storage, transmission, or processing, that introduce unintended changes to the original data. Generally, when data corruption occurs, the file containing the data becomes inaccessible and/or unusable.
Data Integrity	The accuracy, completeness and consistency of data stored in an information system, free from either accidental or deliberate, but unauthorized insertion, modification or destruction of data in a database.
Disaster	In the context of information systems, 1. An emergency or other event resulting in the destruction, theft, or corruption of data. 2. An inability to access an information system and/or its data for longer than a reasonable

	period, the duration of which is determined by the criticality of the system resources and data. 3. Extensive damage inflicted on an information system, the availability of which is necessary for the maintenance of confidentiality, integrity, and availability of data required for the operation of an organization.
Disaster Recovery	The process, policies, and procedures preparing for recovery or continuation of the technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery includes planning for resumption of operating system and application software, data, hardware, and communications (networking).
Distributed system	An information system composed of multiple autonomous computers that communicate through a computer system.
POPIA	To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.
Hacking	Detecting weaknesses in a computer or computer network. Hacking tools are programs designed to assist with hacking; these programs are often malicious and may be used to detect and exploit vulnerabilities in operating systems and/or user accounts.
Information system	An integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, communications, and digital products, support, and services.
IT	Information Technology
IT resources	All Smartcall system computing facilities, equipment, hardware, software, data, systems, networks and services that are used for the support of the teaching, research and administrative activities of the Smartcall System
Maintenance window	The period of time designated in advance by a technical staff during which preventive maintenance that may cause disruption of service will be performed on an information system.
Network/system topography	Describes the arrangement of systems on a computer system, defining how the computers, or nodes, within the system are arranged and connected to each other.
Non-technical controls	Management and operational controls such as security policies, operational procedures, and personnel, physical, and environmental security.

Preventive maintenance	A form of system maintenance conducted on a regular basis and intended to maintain and/or improve information system performance, avoid unplanned downtime, keep system software programs up-to-date, and prevent problems from occurring on an information system.
Protected data	Any data governed under federal or state regulatory or compliance requirements (such as the POPIA), as well as data deemed critical to the Smartcall business processes which, if compromised, may cause substantial harm and/or financial loss.
Residual risk	As it pertains to Smartcall IT, any risk (vulnerability or exposure to loss or harm) that remains after mitigation of a risk or risks identified through the security risk assessment process.
Restricted data	Highly sensitive information intended for limited, specific use by individuals, workgroups, departments, or organizations with a legitimate “need to know.” On USF System information systems, data stored digitally that requires restrictions to its access and dissemination, as defined by the (POPIA), or by Smartcall policies and standards.
Risk	The probability that a particular vulnerability or vulnerabilities in the Smartcall information system will be intentionally or unintentionally exploited by a threat which may result in the loss of confidentiality, integrity, or availability, along with the potential impact such a loss of confidentiality, integrity, or availability would have on Smartcall operations, assets, or individuals.
Risk analysis	The process of identifying the most probable threats to Smartcall information systems, revealing how frequently particular undesired events occur, and of determining the criticality, causes, and consequences of these threats and/or events.
Risk assessment	The overall process of risk analysis and risk evaluation and a key component of risk management that involves identifying and evaluating
Risk evaluation	The process used to determine priorities for risk management by comparing the level of risk against predetermined standards, target risk levels, or other criteria.
Risk management	The overall process for identifying, controlling, and mitigating security risks to information systems. Smartcall System IT risk management comprises risk assessment, risk analysis, and treatment of risk, and includes the selection, implementation, testing, and evaluation of security controls.
Risk mitigation	The systematic reduction in the degree of exposure to a risk and/or the probability of its occurrence.
Security	In IT, the preservation of confidentiality, integrity, and availability of an information system and/or the data that resides on it.
Security authorization	The official management decision made by a senior organizational official to authorize operation of an information system and to accept certain risks to organizational operations and assets,

	individuals, and other organizations based on the implementation of an agreed-upon set of security controls.
Security incident	Any computer or network-based activity that results (or may result) in misuse, damage, or loss of confidentiality, integrity or availability of an information system and/or the data that resides on it.
Sensitive data	Any data which, if compromised with respect to confidentiality, integrity, and/or availability, could have an adverse effect on the organization's interests, the conduct of its programs, or the privacy to which individuals are entitled.
Sensitivity	A measure of how freely data stored on an information system can be handled.
Software patch	An update that fixes bugs (errors, flaws, mistakes, failures, or faults), increases security or adds new features to a software program. A patch typically does not include substantial enough changes to warrant a new version or release of the entire program.
Software update	Modification to an existing version/release of a software program to develop or improve upon its features, function and/or performance without upgrading it to a new major version.
Software version upgrade	Replacement of a software program with a newer version of the same program in order to bring it up to date or to develop or improve upon its features, function and/or performance.
Storage area network	A dedicated system that provides access to consolidated, block level data storage; a system with the primary purpose of transferring data between computer systems and storage elements.
System development life cycle (SDLC)	A conceptual model used in project management that describes the phases involved in an information system development project. A typical information system life cycle includes these phases • Initiation – the system is described in terms of its purpose, mission, and configuration. • Development and Acquisition – the system is constructed according to documented procedures and requirements • Implementation and Installation – the system is installed and integrated with other applications, usually on a network. • Operational and Maintenance – the system is operating and maintained according to its mission requirements. • Disposal – the system's life cycle is complete; it is deactivated and removed from the network and active use.
System integrity	The state or quality of an information system when its intended functions are performed in an unimpaired manner, free from either intentional or accidental, but unauthorized manipulation, changes or disruptions.
System maintenance	The adjustment or modification of an information system to correct faults, improve performance, adapt to change in requirements, or changes in the system environment.

System management	The administration/oversight of a distributed computer system, which may include development, configuration, maintenance, and security and contingency planning.
Technical controls	Safeguards that are incorporated into computer hardware, software, or firmware, such as access control mechanisms, identification and authentication mechanisms, encryption methods, and intrusion detection software.
Threat	Any circumstance or event that has the potential to intentionally or unintentionally exploit a particular vulnerability in the USF Health information system, resulting in a loss of confidentiality, integrity, or availability.
Vulnerability	A flaw or weakness in the Smartcall information system security procedures, design, implementation, or internal controls that could be accidentally or intentionally triggered or exploited and result in a security breach or a violation of the system's security policy.

Table of Contents

1. Introduction

The Smartcall IT Security Plan defines the information security standards and procedures for ensuring the confidentiality, integrity, and availability of all information systems and resources under the control of Smartcall Information Technology. Included are:

- Definitions and descriptions of terms and acronyms used in the Smartcall Security Plan and related documentation.
- The roles and responsibilities of individuals and groups within the Smartcall System.
- Descriptions of or links to descriptions of standards and procedures for:

    - Security
        - Physical Security
        - Hardware/Software/Patching
        - Access Controls
        - Disaster Recovery
        - Business Continuity

    - Staff Obligation
        - Acceptable use Policy
        - User Access Control
        - Authentication
        - Media Management

    - Security concerns in system management (PLACE HOLDER)

The Smartcall IT Security Plan supplements the Official Security Policies, Standards, and Procedures that have been established for the Smartcall System. This security plan is intended to comply with the regulations and policies set down by the Republic of South Africa, Smart Phone (Pty) LTD t/a Smartcall, and the Protection of Personal Information Act (POPIA) as per the requirements of lawful personal information processing prescribed by the Protection of Personal Information Act.

2. Scope

The standards and procedures set down in the Smartcall IT Security Plan apply to all information systems and resources connecting to the Smartcall System network.

3. Roles and Responsibilities

These are specific individuals or groups within the Smartcall environment and their responsibilities in relation to Smartcall's security standards and procedures.

IT Manager – Responsible for providing information technology management, development, planning, procurement and implementation activities related to the delivery of quality information services and products for both the business and .
Incident Response Team (IRT) – With a primary goal of protecting the overall computing infrastructure of Smartcall and Vodacom. The IRT is responsible for responding quickly to

identify threats to the data infrastructure, assess the level of risk (Standard, Medium, High), and take immediate steps to mitigate risks considered significant and harmful to the integrity of Smartcall/Vodacom information system resources. IRT members notify the appropriate department leads of any incident involving their resources.

Database Administrator - Maintains a successful database environment by directing or performing all related activities to keep the environments data secure. The top responsibility of a DBA professional is to maintain data integrity. The DBA will ensure that data is secure from unauthorized access but is available to users, as per the internal access request policies withing Smartcall.

Development – Responsible for ensure that code and processes that go into developing applications are as secure as possible, thorough testing and evaluation are required at each step of development. All data captured externally is processed and stored with strict control.

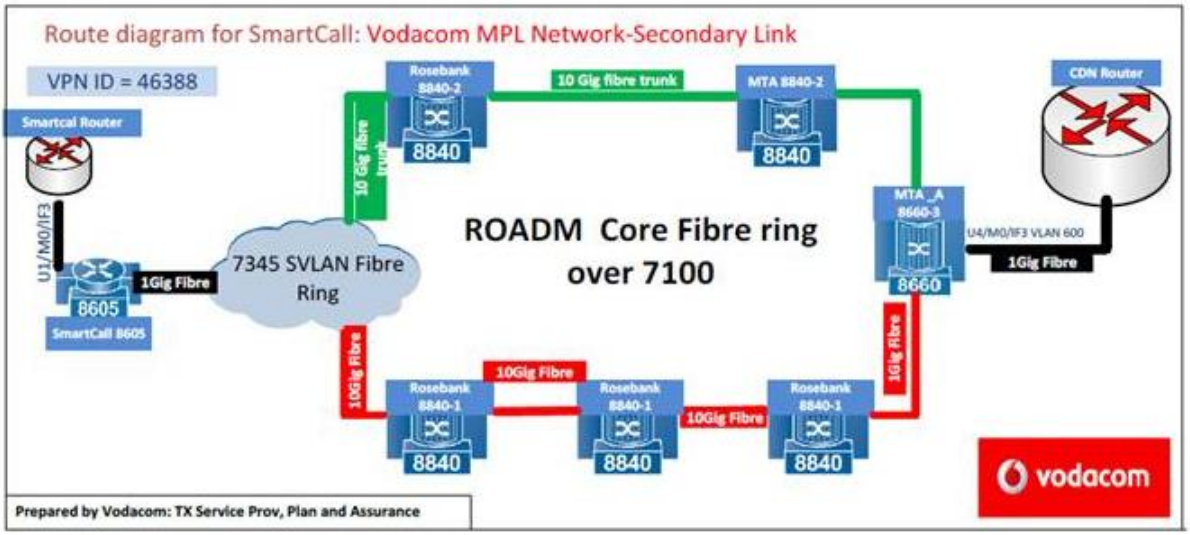
4. Standards and Procedures

Smartcall maintains the highest level of security with regards to Vodacom data. This level of security is further maintained through progressive policies that are enforced, evaluated and maintained on a regular basis.

To further improve this security posture, a direct 1:1 link was installed between Vodacom and Smartcall, this gives Smartcall the ability to follow similar internal security measures as implemented by Vodacom South Africa, to ensure users are vetted and granted access on a strict requirement only basis.

Current connection Topology Smartcall – Vodacom:

Primary Link – Smartcall to Vodacom
Secondary Link – Smartcall to Telkom to Vodacom (This phase is in revision to accommodate fiber connectivity)



4.1. Security

Smartcall utilizes a number of security systems designed to help fulfil its security mission. These systems complement the policies, procedures, and measures that form part of Smartcall's robust security program.

4.1.1 Physical Security:

- **Perimeter:** Fencing/Electric Fencing is the first layer of security. Access points/gates are secured through one of the following methods: Automated gates through the use of proximity cards that will allow the user basic access to the premises. All perimeters and access points are monitored 24/7 by CCTV and on-premise security guards.

- **CCTV:** Over 50 Cameras have been deployed in our environment, and are strategically placed throughout. The onsite data centre is monitored by 3 always-on camera systems that give security and IRT teams the ability to monitor access. Alert based recognition has been implemented to further notify security teams of unauthorised access in the event of a breach. CCTV systems are monitored 24/7 and recordings can be accessed at anytime.

- **Access Control:** Access Control systems have been installed throughout the environment. These biometric and card based access points secure doors to buildings, and access gates. Security is able to effectively track and control access. Each employee and contractor is required to wear an identification/access badge which is individually tailored for specific access. An access request form is required to access any area higher than level 2 access.

  The data centre is protected by triple layer authentication. The first layer requires the accessing user to enter in an access pin, the second layer requires the accessing user to enter another pin that is changed every 30 days, and lastly the third layer, the accessing user is required to either use an access card with Level 4 access or have level 4 biometric access granted in order to access the data centre.

- **Intrusion alarms:** Intrusion alarms are utilized throughout the buildings. These alarms provide 24/7 monitoring in remote locations where staff is not always present. The alarm sensors include door/window contacts, motion detection, and glass break systems.

- **Cabinet Control:** All server cabinets are locked and only upon the required approval from management are authorized personal allowed to access a specific cabinet. An access form must be filled out and logged on the internal helpdesk ticketing system.

4.1.2 Hardware/Software Security/Patching:

- **Hardware Software Monitoring:** Each data storage platform or database that houses user data is secured by an on-premise Host-based Intrusion Prevention System (HIPS). This system protects the environment from malware and unwanted activity attempting to negatively affect the environment. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys.

  Databases are also further protected by the use of activity monitoring sensors that will alert both the database administrator and relevant IT teams.

- **Software Security:** Throughout the environment both servers and user machines are protected with antivirus software as well as monitoring software. Triggers are set up on machines to inform response teams of any warning or critical activity being carried out.

- **Patching:** Smartcall maintains appropriate and timely updates, patches and maintenance to ensure that systems and data are adequately protected. Critical updates/fixes should be applied as soon as is possible in accordance with institutional approval and sign-off procedures.

  Enterprise Information Systems Covered By This Policy:

  - Operating System (OS) updates for servers, workstations, and other end user equipment is installed in a timely manner in accordance to environment needs and requirements in order to minimize and avoid exposing the organisation to risks.

  - End-user applications regular and critical updates should be installed in a timely manner in accordance to environment needs and requirements in order to minimize and avoid exposing the organisation to risks.

  - Network infrastructure and systems regular and critical updates are installed in a timely manner in accordance with environment needs and requirements in order to minimize and avoid exposing the organisation to risks.

  - All other enterprise information systems and components regular and critical updates are installed in a timely manner in accordance to environment needs and requirements, and to minimize and avoid exposing the organisation to risks.

4.1.3 Access Controls

Controls are in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the Smartcall system. Data used for authentication shall be protected from unauthorized access. Controls are in place to ensure that only personnel with the proper authorization and a need to know are granted access to Smartcall's systems and their resources. Remote access shall be controlled through identification and authentication mechanisms after approval.

4.1.4 Disaster Recovery

To meet the organizations business objectives, respond to a major incident or disaster, and restore the organization's critical business functions, Smartcall shall adopt and follow well-defined and plans and procedures.

This Disaster recovery policy is required to respond to a major incident or disaster by implementing a plan to restore Smartcall's critical business functions.

Appendix A - Reference Document: Smartcall Disaster Recovery Plan (DRP)

4.1.5 Business Continuity

This Continuity/Contingency Plan establishes procedures to recover Smartcall services following a disruption.

The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    - Notification/Activation to detect and assess damage and to activate the plan.
    - Recovery to restore temporary operations and recover from damage.
    - Reconstitution of systems and normal operations.
- Identify the critical activities, resources, and procedures needed to carry out operations during prolonged interruptions to normal operations.
- Assign responsibilities to designated personnel.
- Provide guidance for recovering operations during prolonged periods of interruption to normal operations.

The intended audience of the Smartcall Business Continuity/Contingency Plan is the IT Manager, Incident Response Team, Project Sponsor (Vodacom), procurement officer/office, and any senior leaders whose support is needed to carry out acquisition plans.

Appendix B - Reference Document: Business Continuity Plan - External (25 March 2019)

4.2. Staff Obligation

Access to computer systems and networks owned and operated by Smartcall is a privilege which imposes certain responsibilities and obligations of the user. The objective of this policy is to ensure an available, reliable, data secure and responsive network environment at Smartcall. It is the responsibility of each user to ensure that they understand and abide by the company code of conduct as well as the various standards and IT policies in place to protect the organization from damage.

4.2.1 Acceptable User Policy:

Any activity that compromises the performance of Smartcall's computers and/or network such that others are negatively affected is not acceptable. Users are required to ensure they regularly revise existing policies on security and data control per department. Any user that violates or ignores these requirements will be subject to disciplinary hearing, followed by an extensive re-training initiative to ensure compliance.

4.2.2 User Access Control:

All users within the Smartcall environment are issued access level based on their roles and job functions.

Access requests to information or applications can be defined as 4 Levels of Access:

- **Level 1** - Role-Based Access Control (RBAC) – Users are given role based access that allows them to perform their job function.
- **Level 2** – Elevated access is granted after an access request form is filled out and once approved the permission is assigned. Permissions are revoked after a 30 day period.
- **Level 3** – Level 3 Access is for 3rd party vendors who require access to certain parts of Smartcall, this is always done under the supervision of a Smartcall IT employee. The Smartcall employee will perform all the terminal required tasks as per the vendor's instruction. Under no circumstances is data exposed or exchanged.
- **Level 4** – Access on this level is granted to employees that need to access sensitive business data, an access document needs to be signed and approved by both the acting department manager, IT Manager and the Director of the organisation.

All access requests are logged and stored on the internal Helpdesk platform, all physical requests are allocated a Helpdesk reference number and a filed for a period of five (5) years

Appendix C - Reference Document: Smartcall IT Security Standard
Appendix D – Reference Document: Smartcall Access Request

4.2.3 Authentication:

All users on the Smartcall network require User Authentication and User Authorization. Active Directory user authentication confirms the identity of any user trying to log on to a domain. After confirming the identity of the user, the user is allowed access to level 1 resources.

Single sign on capability is disabled by to ensure that users are required to enter in a new password so they can authenticate that user for that application or platform session.

Appendix C - Reference Document: Smartcall IT Security Standard

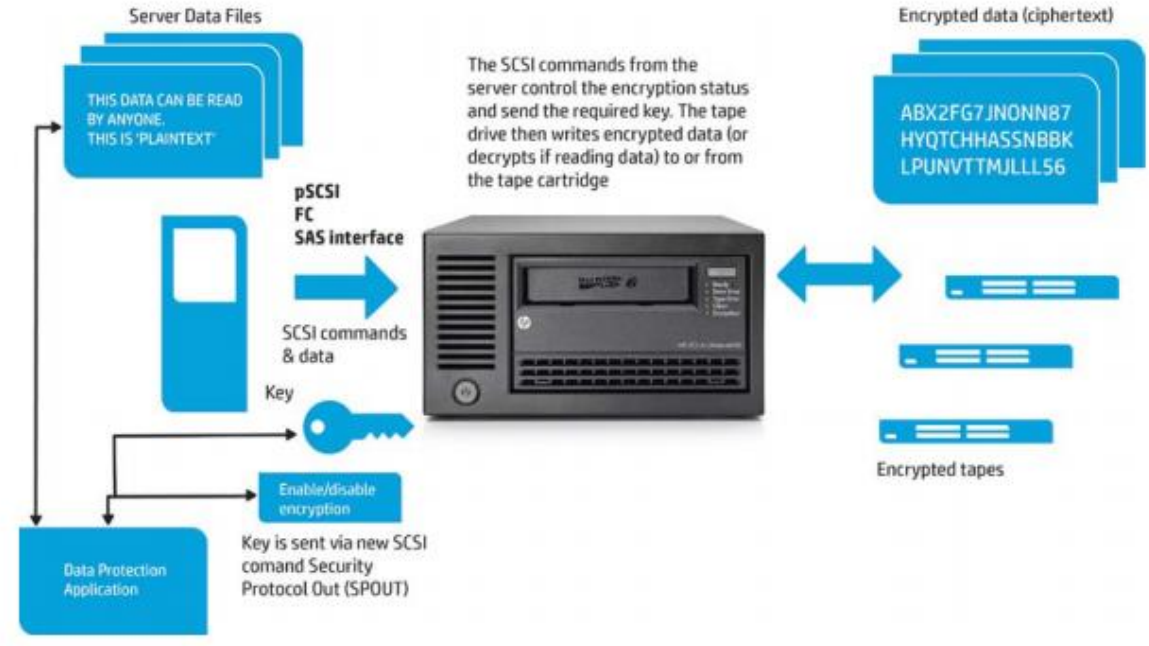
4.3. Management of Media

All backed up media and data withing the Smartcall environment is encrypted and stored in a secure, geographically separate location from the original as well as being isolated from environmental hazards. Sets are allocated in daily, monthly, weekly and yearly. Access is monitored and granted to IT support staff for that week and is then rotated to a new IT support staff member the following week.

Full and incremental backups preserve corporate information assets and are performed on a regular basis for audit logs and files that are irreplaceable, have a high replacement cost, or are considered critical.

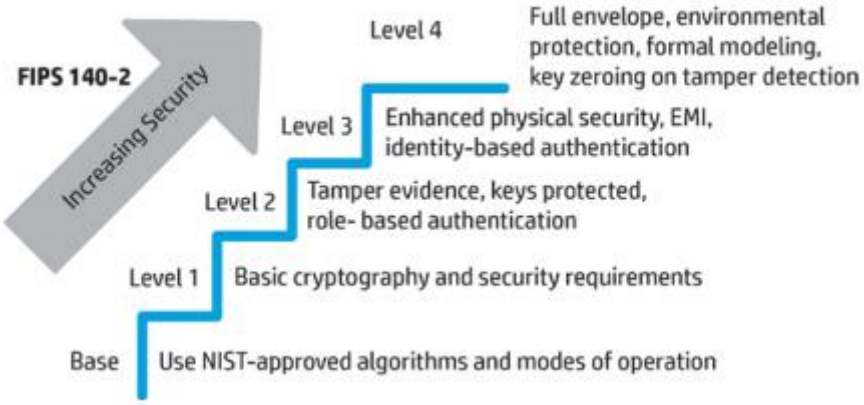
All data is encrypted through the use of HP StoreEver LTO Ultrium hardware.

This process is demonstrated below and forms part of our active security infrastructure to protect moving data.



Before media leaves our secure storage area. The tapes are documented and a time stamp provided. Before the IT staff member can scan the tapes and prepare them for use, an inventory of the tape media needs to be initiated. This checks the validity of the tapes and ensures the correct tapes are being allocated before the new data can be written to them. This allows us to quickly find and restore data based on the file registry and tape information.

All HP LTO-6 Ultrium Tape drives and tapes used in our environment are level 1 and Level 2 FIPS 140-2 compliant



Appendix A - Reference Document: Smartcall Disaster Recovery Plan (DRP)
Appendix C - Reference Document: Smartcall IT Security Standard

4.4. Record Keeping

Place holder