Document number: T.4
Document Name: IT Operations Systems Security Policy
Document Owner: Operations Director
Issue Date: 01/05/2024
Current Revision Date: 01/05/2024

prevision research
THE DATA COLLECTION EXPERTS

IT Operating Systems Security Policy

Objective and Scope

Operations systems security is intended to ensure correct and secure operations of information processing and management facilities and activities.

This scope includes:

- Systems architecture and documentation
- Systems protection during development activities
- Change and capacity management
- Protection from malware
- Systems backups
- Redundancy of information processing facilities
- Logging and monitoring operational activities

Refer to:

- ‘Software Applications Assets Management Policy’ for operational software control and technical vulnerability management.
- ‘Documented Operating Procedure’ for standardisation of processes.

Roles, Responsibilities and Authorities

The Operations Director or competent IT Team delegate takes ownership of documenting and maintaining current operating procedures including change management and ensuring they are communicated to relevant interested parties including in-house and outsourced provisions as required.

A designated IT officer shall be nominated by the Operations Director to monitor systems capacity requirements including capacity when undergoing operational change processes.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted

IT Operating Systems Security Policy

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents
Online Safety Act 2023	https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
Modern Slavery Act 2015	https://www.legislation.gov.uk/ukpga/2015/30/contents/enacted
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Operations	8.1			
Change management		12.1.2		8.32
Capacity management		12.1.3		8.6
Separation of dev/test/ops environment		12.1.4		8.31
Malware protection and controls		12.2.1		8.7
Information backup		12.3.1		8.13
Redundancy of information processing facilities				8.14
Logging and monitoring		12.4.1		8.15
Logged information protections		12.4.2		8.15
Monitoring activities		12.4.1		8.16
Administrator and operations logs		12.4.3		8.15
Clock Synchronisation		12.4.4		8.17

IT Operating Systems Security Policy

Related Information

- Software Applications Assets Management Policy
- IS within the Physical Working Environment Policy
- Risk Management Procedure
- Information Classification Policy
- White list of acceptable applications

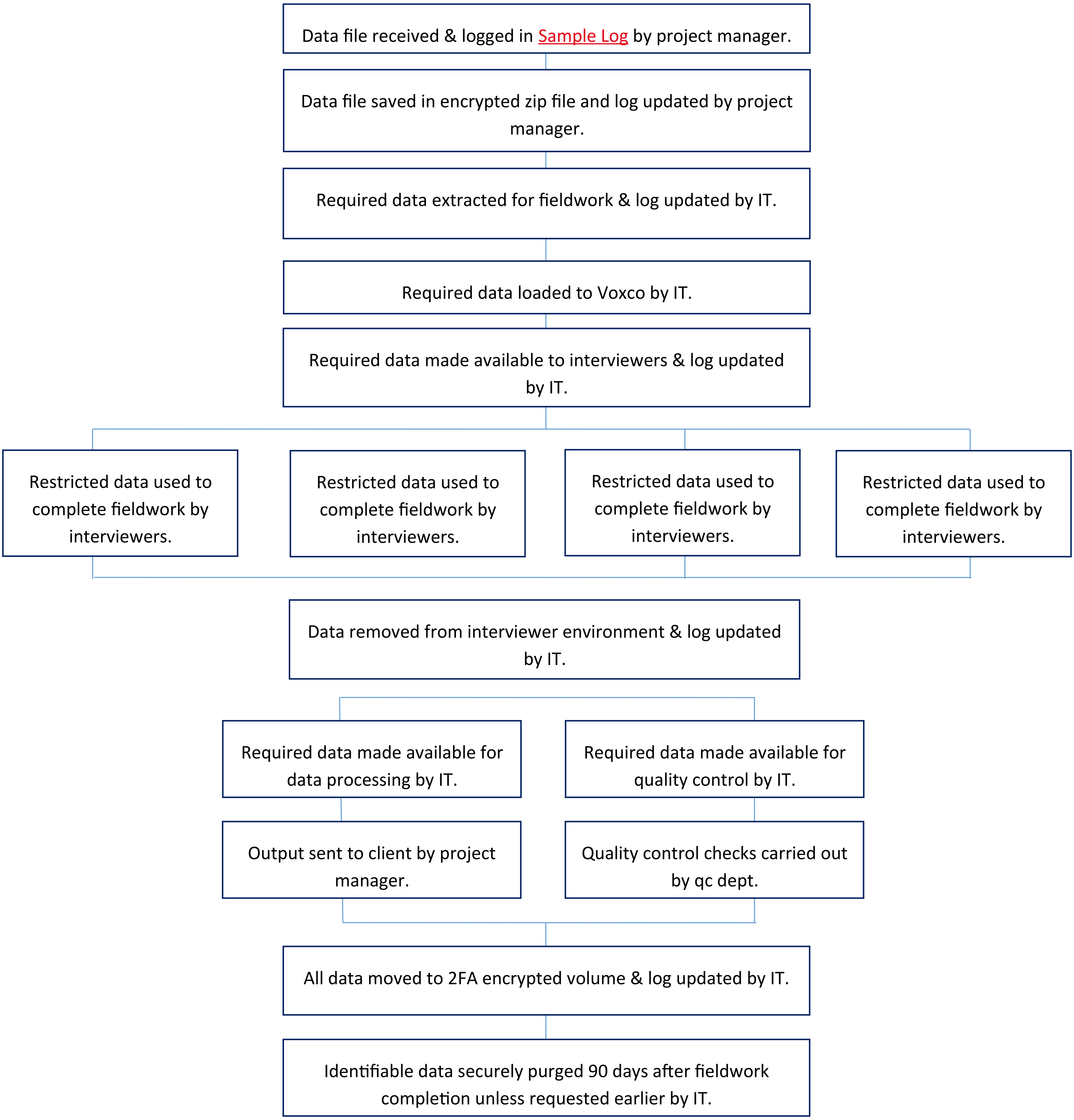
Policy

Prevision Research operational data and information management and workflow processes shall be documented and maintained as current by persons with assigned responsibilities.

Systems in place include protection from malware, backups and logging and monitoring processes.

IT Operating Systems Security Policy

IS Systems life cycle / architectural map



Data file received & logged in Sample Log by project manager.

Data file saved in encrypted zip file and log updated by project manager.

Required data extracted for fieldwork & log updated by IT.

Required data loaded to Voxco by IT.

Required data made available to interviewers & log updated by IT.

Restricted data used to complete fieldwork by interviewers.

Restricted data used to complete fieldwork by interviewers.

Restricted data used to complete fieldwork by interviewers.

Restricted data used to complete fieldwork by interviewers.

Data removed from interviewer environment & log updated by IT.

Required data made available for data processing by IT.

Required data made available for quality control by IT.

Output sent to client by project manager.

Quality control checks carried out by qc dept.

All data moved to 2FA encrypted volume & log updated by IT.

Identifiable data securely purged 90 days after fieldwork completion unless requested earlier by IT.

IT Operating Systems Security Policy

Change management

Any planned or unintended change that has a potential to impact change of system configs, use of privileges, files accessed/type of access, IP addresses, alarms raised, activations, de-activations and records of transactions that affects the business' information security status in any way shall be subject to:

1. A planned risk assessment to determine information security effects of the change. When change is unintended, an immediate risk assessment shall be undertaken to determine what effects have occurred. This process shall identify and record changes.
2. Determine what actions are required to monitor and test changes being introduced (or have occurred) by the change process.
3. Decide whether to progress with actions (risk review) and how this is to occur e.g. document a procedure or project plan. Record approvals to proceed and acceptance by critical interested parties.
4. Before progressing the change, put in place contingency measures for high risk changes in case the plan has to be aborted.
5. Keep an audit log of changes and the change event

Capacity management

Capacity management is about resources (people, infrastructure and technology) planning for future needs to ensure business and information sustainability.

Technology resources

Technological capacity usage monitoring and measurement processes shall be enabled to inform management of capacity availability and flag issues before they become risk critical. Future projections in business development technical resources wear and redundancies must also be considered.

This is a role assigned to an IT competent individual the Operations Director reporting:

1. In real time on a day to day basis
2. Future projections in relation to redundancies and need for upgrades
3. The need to restrict or divert bandwidth within the organisation to better utilise and optimise resources

Housekeeping including deletion of obsolete data, disposal of data post retention period, decommissioning of obsolete or otherwise redundant technologies and effective bandwidth management should be undertaken in a timely manner.

As an outcome of technical capacity management monitoring, any need to review human resources capacity shall also be reported for resources planning purposes.

People resources

Human resources capacity needs shall be taken into account at planning stages, throughout any change management including new projects, new technology and general redundancies. Lead time planning also needs to be considered in recruitment, outsourcing and skills development.

IT Operating Systems Security Policy

Separation of development, testing and operational environments

Prevision Research operational systems are siloed from any activity involving new or changed development work. When undertaking testing of new or changed development works, users must not use their normal profile identifiers to risk contamination of operational systems. Test sites must declare and display their test status at all times.

Before any development work is moved from the development stage to the operational platform:

- separation between development and production/operational sites is determined,
- rules, approvals at key risk points and final authorisations are agreed,
- zero sensitive data is used during development or testing,
- to ensure systems are compatible, a test run is undertaken on a limited siloed operational environment without exposing sensitive or business critical information, and
- further testing is undertaken on a broader sample of various aspects of siloed operational systems, hardware and software to test compatibility and look for anomalies.

Protections of development and test activities include:

- patching and updating the development, integration and test tools,
- control of access to the environment and secure configuration of systems and software, and
- monitoring of the process and backups taken.

Malware protection and controls

Detection, prevention and recovery controls to protect against malware are in place. Protection against malware is based on malware detection and repair, information security awareness and appropriate systems access and change controls.

Prevision Research operates a White List of approved software applications that can be uploaded onto company devices. All other applications should be considered blacklisted (do not use).

Microsoft Defender shall be installed on desktops and laptops to guard against malware attacks with the following features:

- Real-time virus & malware threat detection
- Firewall and network protection
- Ransomware protection

Business continuity plans are in place in the event of a malware attack, including first 5 minute actions to limit the extent of the attack and initiate backup.

Information backup principles

Prevision Research plans and enacts a comprehensive back up, retention and restoration plan based on:

1. Determining what records are required and where they will be backed up remotely to protect them from risk of compromise.
2. Risk rating of records according to criticality to the business and risk of regulatory breach, and provide priority backup arrangements for this data including encryption.
3. Providing a test regime to ensure backups are fit for purpose, free of compromise and able to be restored as planned.

IT Operating Systems Security Policy

Systems backup

Prevision Research backup and storage management applies to data and information, software applications and system images.

This includes:

Operations database maintains a full system backup.

- Nightly database backup by Synology Cloud C2
- Annual test restores to Synology NAS.

Database backups are generally retained for a period of 90 days by Synology Cloud C2:

The following standard management applies to web servers:

- Web servers on which end user data is stored are strictly managed under a service agreement with documented access controls, surveillance and security logs, managed by the Operations Director.

Systems backup audit and testing

Web server infrastructure and applications are subject to:

- Weekly Integrity Checks
- Monthly test restores of backed-up data
- Audit of backup six monthly to ensure functionality.

Retention of client information is retained for 90 days after expiry of contract unless otherwise requested by the client.

Redundancy of Information processing facilities

Prevision Research ensures continuous operation of information processing facilities by:

- Having the ability to duplicate facilities as a business risk mitigation model allowing for backup or restoration as necessary
- Testing the backed-up data to retain its currency and enable restoration in the case of an emergency
- Having monitoring mechanisms in place to provide timely alerts and warnings
- Cloud-based business-critical software to allow for rapid relocation.
- Agreements with partners to support us as necessary

Also refer ICT continuity plans.

Event logging

Prevision Research user event logging and monitoring is undertaken Synology DSM.

Synology DSM describes and provides capabilities including:

- User and device IDs, activities
- date/times successful attempts,

IT Operating Systems Security Policy

Infrastructure logging and monitoring is undertaken through Synology DSM. Real time alerts are communicated through Email. These systems monitor server health and resource utilisation.

Monitoring

Monitoring of logs and server health, network application functionality for both appropriate and inappropriate activities. The system shall flag alerts, actions and risk episodes undertaken using automatic continuous Synology DSM.

This role is assigned to Operations Director for:

- reading and responding to monitoring reports and flags
- escalating to an incident or other event as appropriate
- initiating periodic updates and reviews to senior ITC personnel
- initiating threat intelligence responses.

Post an event or incident requiring an escalation process, a risk assessment will be undertaken to evaluate the effectiveness for the response and look for improvement opportunities.

Administrator and operator logs

Prevision Research operational logging is managed by Synology DSM. Audit logs are read-only and record both user and administrator events with only administrators having view access to logs.

Server infrastructure logging is stored in Synology DSM and managed by Prevision Research. Logs are read-only.

Log analysis

Prevision Research undertakes an analysis of log events to inform the reader of any unusual activity, anomalies, risk to regulatory compliance or suspected unauthorised changes.

Given the nature of log information being data secure and PII or business sensitive, only persons with the appropriate CIA security clearance may review or analyse logged data.

Analysis shall seek to determine IS threats, vulnerabilities, suspected intrusion attempts, actual intrusion, patterns of abnormal behaviour internally or externally and outsourced provider activities.

Should the need arise from the analysis process, and escalation may occur in which case, the ISMS Representative, IT Representative and Privacy Officer shall be informed and a subsequent investigation shall be enacted.

Clock synchronisation

Prevision Research clock synchronisation is managed server side where logging is collected, including the use of 3rd party logging tools. Servers are reviewed annually to ensure clocks are synchronised with the network time protocol.

The following servers / services are used:

- Synology DSM - pool.ntp.org

IT Operating Systems Security Policy

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change failure or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N