

# CoverImage_governmentIT Security and Governance

IT Security Policy & Procedure Specification Document 2019-2020

# Zoodata Data Security Policy

## Purpose

Zoodata shall comply and shall ensure that any sub-contractor complies, so far as compliance is required, with the secrecy and security requirements of the Customer as set out in the Official Order, or notified by the Customer to the Contractor from time to time.

## Application

All employees and agents of Zoodata, with particular reference to:

1. Zoodata development personnel
2. Zoodata Dev/ops personnel

This policy applies to the following areas:

1. Security Management
2. Security Risk Management
3. Security Policies and Procedures
4. Information Access
5. Security Obligations
6. Security Training and Awareness
7. Business Continuity Management
8. Contracted Service Providers
9. Government Services
10. Security Plans
11. Compliance
12. Information Value
13. Information Management
14. Information Sharing
15. Personnel Lifecycle
16. Information Communications Technology (ICT) Lifecycle
17. Physical Lifecycle

Table of Contents

[IT Security and Governance 1](#_Toc23327125)

[Zoodata Data Security Policy 2](#_Toc23327126)

[Purpose 2](#_Toc23327127)

[Application 2](#_Toc23327128)

[Introduction 4](#_Toc23327129)

[Policy Requirements 4](#_Toc23327130)

[Security objectives 4](#_Toc23327131)

[Information security controls 5](#_Toc23327132)

[Access control 5](#_Toc23327133)

[Passwords and Authentication 5](#_Toc23327134)

[Privileges 5](#_Toc23327135)

[Individual Access Accounts 5](#_Toc23327136)

[Group / Generic Logon Accounts 6](#_Toc23327137)

[Single sign-on arrangements 6](#_Toc23327138)

[Cloud services 6](#_Toc23327139)

[Cyber threats and malware 7](#_Toc23327140)

[Data encryption 8](#_Toc23327141)

[Data storage, transfer and disposal 8](#_Toc23327142)

[Mobile devices and computers 10](#_Toc23327143)

[Remote Access of Zoodata Information via VPN 11](#_Toc23327144)

[Network Security Management 11](#_Toc23327145)

[Personnel Security 11](#_Toc23327146)

[Physical Security 12](#_Toc23327147)

[Security Continuity 13](#_Toc23327148)

[Backup and Disaster Recovery 14](#_Toc23327149)

[Security Incident Management 14](#_Toc23327150)

[Software Licensing, Installation, and Use 15](#_Toc23327151)

[System Acquisition, Development, and Maintenance 15](#_Toc23327152)

[Teleworking and Remote Access 16](#_Toc23327153)

[Third Parties and Supplier Relationships 16](#_Toc23327154)

[Compliance, Monitoring, and Evaluation 17](#_Toc23327155)

[Definitions 18](#_Toc23327156)

# Introduction

The Zoodata IT Sceurity Policy and Procedure Specification Document provides the policies and procedures for selection and use of IT within the business which must be followed by all staff. It also provides guidelines Zoodata will use to administer these policies, with the correct procedure to follow.

Zoodata will ensure all IT policies are kept current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures are binding to all employees and agents of Zoodata. This includes any person working in a permanent, temporary, casual, contracted, termed appointment or honorary capacity.

# Policy Requirements

Implementation of the policy requirements should be done using an appropriate risk-based approach and without impacting service delivery to clients. Exceptions to implementation require appropriate approval from senior management.

A consistent approach must be applied to the management of information communication technology risks, and to the identification and management of information security risks. Further, Zoodata employees and agents should identify and manage information security risks in accordance with the Zoodata Risk Management Policy to the extent they are able.

Security risks are to be recorded by staff as soon as they are identified, and the relevant procedure must be followed depending on the level of the issue. Issues must be reported and recorded within 6 hours of identification.

Security objectives

The following objectives apply to Zoodata digital information and systems:

* Confidentiality – the treatment of information that an individual or a business has disclosed in a relationship of trust and with the expectation that it will not be used or divulged to others in ways that are inconsistent with the understanding of the original disclosure, without permission.
* Integrity – data is protected against unauthorised alteration or destruction and any challenges to information authenticity are prevented, giving clients confidence in the way Zoodata protects and handles information.
* Availability – authorised users are provided with timely and reliable access to information and systems for authorised purposes.
* Privacy – the right or expectation of the individual or business that their information (identifying or otherwise) will not be disclosed to any third party without consent.

Information security controls

Zoodata has processes in place to support the following information security controls.

Access control

Access to the Zoodata system information and information processing facilities must be controlled and limited, in accordance with the following overarching principles:

* Need-to-Know and Need-to-Use principles: users are only granted access to the information or information processing facilities they need to perform their tasks.
* Principle of Least Privilege: only the minimum privileges necessary to complete required tasks will be assigned to each user.
* Segregation of Duties (or Separation Principle): the granting of roles, duties and associated access rights must be sufficiently segregated to minimise risk and avoid conflict of interest

Passwords and Authentication

All Zoodata system access accounts must be protected with strong passwords, or other secret authentication information, to validate the identity of an entity accessing, providing information or undertaking a transaction. Strong passwords as defined by industry best practice are to be applied wherever the system allows. Passwords must remain confidential at all times and be securely stored using encryption.

### Privileges

Processes for the management and use of allocated privileges must be established that comply with the following standards and requirements:

* Privileges assigned to each individual are to be monitored by line managers and data custodians, and modified or revoked upon a change in individual status with the organisation. These privileges are also to be reviewed at regular intervals using a formal process to ensure they are complete, accurate and access is still required.
* The network access rights of all staff members are to be removed upon termination of their employment or contract. Staff responsible for managing other staff members must ensure those exiting the organisation have their access immediately revoked, by initiating and approving an Access Request Form prior to exit. Regular reviews of inactive accounts, as an established process, are required.
* Privileges should be role based rather than individual specific
* Individuals requiring highly privileged access (eg system administration / super user access) rights are to be assigned a different user identification (ID) for this purpose, which is separate from their user ID used for regular business activities. Regular business activities should not be performed using highly privileged IDs.

### Individual Access Accounts

A formal user registration and termination process must be established to grant access by individuals to the WA health system’s information systems that complies with the following:

* Approval for access to be provided by authorised personnel, consistent with the relevant policies.
* A unique identified is to be assigned to each individual or business which has a specific need to access Zoodata systems.
* All internal requests for access are to be approved by senior management.
* For non-permanent staff members, user accounts to be set to expire in accordance with the contract expiry date.
* All individuals must sign a Non-Disclosure Agreement with Zoodata and a copy of this agreement must be maintained.
* Where access to systems is provided via swipe card technology, individuals must immediately report any lost or stolen system access/swipe cards to ensure access can be de-provisioned immediately.

Group / Generic Logon Accounts

Group / generic logon accounts (ie accounts created for more than one individual to use) are not permissible without the documented approval of senior management staff. Where approved, the relevant management staff member remains accountable at all times for the access to the information via that group / generic logon account and will ensure:

* procedures are developed to ensure passwords are updated as appropriate, confidentiality is maintained, and usage can be monitored;
* a regular monitoring and audit process is in place;
* a risk assessment is undertaken and mitigation strategies in place to prevent any accidental or intended shared use of application logons, particularly where single sign-on arrangements are enabled for workstations. These strategies may include shorter application timeouts (where possible) and/or stringent guidelines for use;
* procedures are in place for highly privileged or administrator group / generic logon accounts to ensure the account is used for its intended system configuration capabilities only; and
* all accounts are reviewed by the relevant management staff member at regular intervals using a formal risk-based process to ensure they are still required and the appropriate approvals for use exist.

### Single sign-on arrangements

Relevant Zoodata personnel must ensure single sign-on access arrangements have controls in place to maintain information security, particularly in relation to any additional risks associated with shared workstations. These may include, but are not limited to, appropriate application timeouts, standards and guidelines for implementation and use, and clear user identifiers/banners.

Cloud services

Prior to implementing cloud computing models for Zoodata systems, Zoodata must ensure the following requirements are met:

* Comprehensive risk assessments are to be conducted involving not only information security risks but also consideration of the jurisdictional, governance, privacy, data ownership, data sovereignty, financial, technical, and legal risks. These risks must be compared against an objective risk assessment of using in-house computer systems.
* Service Providers are to conduct risk assessments in consultation with technical, business and appropriate legal expertise. Zoodata should conduct risk assessments in consultation with technical, business and appropriate legal expertise.
* Consideration must be given to the classification level of the data) and any additional requirements that may be associated with confidential or personal information. If confidential or personal information is to be stored, legal advice should be obtained as part of the risk assessment.
* Agreements with cloud service providers are in place that ensure:
  + the relevant Service Provider or Zoodata has ownership of Zoodata system information;
  + the relevant Service Provider or Zoodata knows the information storage site(s);
  + information retention and disposal is in accordance with relevant recordkeeping plans and retention and disposal schedules;
  + if personal information is to be stored, additional security arrangements are in place to protect and prevent misuse of the information;
  + data is encrypted when at rest (not in use), and cryptographic keys are managed by the Service Provider or Zoodata.
* Legal advice and guidance on all the above points must be sought by Service Providers, or Zoodata prior to procuring and implementing any cloud-based services.

### Cyber threats and malware

All Zoodata information systems (including third party managed systems attached to the Zoodata network) require security controls to be in place to prevent the exploitation of technical vulnerabilities from cyber threats and malware. These should be implemented by Service Providers, Zoodata and Contracted Agents of Zoodata. Cyber security planning, processes and procedures that include detection, prevention, reporting and management of incidents must be implemented. These plans, processes and procedures must contain the elements outlined below.

* Intrusion detection and prevention services that are monitored 24 hours a day / 7 days a week and include the ability to conduct audit analysis and system integrity checking.
* Technical vulnerability scans that have items identified and patched in a timely manner, adequate patch testing and patch testing documentation that is maintained and periodically reviewed.
* Reporting mechanisms to assess and take remedial action.
* Systems in place to receive early warnings of alerts, advisories and patches.
* Where the system allows, mobile devices connecting to the network must be compliant with current anti-malware requirements and scanned regularly.
* Security patches provided by vendors must be installed in a timely manner to mitigate vulnerabilities and guard against cyber threats. Service Providers and Zoodata must have standard change control processes with outage notification and scheduled windows to apply these patches. In cases where an urgent security patching is required, the standard process must be accelerated and out of band changes arranged with the business.
* Where a system is unable to be patched and maintained within appropriate security best practice, containment strategies need to be applied to minimise the risk to the remainder of Zoodata systems. Costs associated with identifying, purchasing and implementing these containment strategies are to be borne by the Service Provider or Zoodata, based on the status and ownership of the system.
* Border gateway services (also referred to as network firewalls) must be reviewed at regular intervals, in line with a risk-based approach for replacement / or upgrade. Border gateway services must be intrusion tested regularly (see dot point one in this section).
* Anti-malware service by Service Providers for externally managed systems and applications.

### Data encryption

Where possible and practicable, encryption must be used to protect the security of WA health system information at rest and in transit. Specifically,

* Data at rest: confidential or health information must not be held on portable storage devices, including mobile phones, unless it is protected by current industry best practices encryption. Passwords must also be securely stored using encryption. Data at rest in applications and medical devices (e.g databases) must be encrypted where possible.
* Data in transit: confidential information must not be transmitted over the internet, public switched telecommunications networks, or unsecured wireless networks, unless the transmission of this information is protected by encryption or other approved secure methods as per this document. Examples of controls include the use of public key infrastructure, secure file transfer, encrypted USB and mobile devices and email encryption.

The section on Data storage, transfer and disposal outlines secure USB and secure file transfer solutions available for use in the WA health system. To maintain the security and integrity of encryption keys, and prevent data loss, an encryption key management process must be developed, implemented and managed by Service Providers, Zoodata or Contracted agents of Zoodata in accordance with the section on Applicability. This process should cover the management lifecycle of generating, storing, archiving, retrieving, distributing, retiring and destruction of keys

### Data storage, transfer and disposal

The storage, transfer and disposal of health information must be undertaken in accordance with its sensitivity and risk profile and protected in accordance with the security controls listed below

#### USB devices

Only Zoodata approved USB devices are to be connected to the Zoodata system information and ICT environment in order to protect the Zoodata system from malicious codes and viruses. These encrypted USB devices are safe to use and display the Zoodata logo on the side of the unit for easy identification. The use of non-Zoodata system USB devices in the Zoodata system network is prohibited and a breach of security.

#### Data storage

* All Zoodata system information must be hosted, transacted, processed and supported in data centres that are connected by high bandwidth, low latency communications, and supported by reliable infrastructure and utilities. The relevant contracting entity has a responsibility to ensure appropriate measures are in place to protect the data. Contracted arrangements must specify the responsibilities of all parties in protecting confidential information to an appropriate level.
* Workstation computer hard drives must not be used as primary or permanent storage for confidential information. Where these hard drives are used for temporary storage purposes, data must be subject to stringent security controls. Confidential or personal data should not be stored on workstation hard drives.
* Printers, facsimile machines and other devices that output confidential or personal information must be subject to security controls. These controls can include physical location in secure areas, PINs/password controls and/or oversight by personnel. Printing from systems containing high risk or classified data should not occur without PIN or password controls. Where this is not possible, appropriate physical security measures must be implemented to protect the information. Where output devices store information on internal hard drives these must be destroyed in accordance with the section on Disposal of storage media
* Where portable devices are used for the capture or transport of original data, such data must be transferred to a primary storage facility as soon as practicable. Confidential or personal information (including digital images, downloaded patient data, commercially sensitive information etc) must not be held on portable devices unless the device is protected by approved cryptography (e.g. USB devices) Individuals are responsible for the security of the devices at all times, including:
  + the secure storage, backup, transmission, access and disposal of information contained on the devices;
  + ensuring they are not left unattended or unsecured at any time;
  + all use is appropriate and by authorised employees or contractors only (i.e. not used by friends, family or other non-approved staff).

#### Data transfer

When information is transmitted outside of the Zoodata system network (e.g. sent via email, SMS or social media over the internet, public switched telecommunications networks or unsecured wireless networks), it is considered unsecured information in transit. Confidential information must not be transmitted through unsecured channels without the use of appropriate cryptography. Transferring personal information may also require specific approvals. Any media containing information must be protected against unauthorised access, misuse or corruption during transportation.

#### Disposal of storage media

Storage media maintained by or for Zoodata systems that is no longer required must be disposed of in a secure manner appropriate to the sensitivity of the information. Data contained in physical media or equipment must be removed using appropriate data sanitisation methods at the time of decommissioning ICT equipment (including mobile phones). The only approved sanitisation and destruction methods are:

* physical destruction of the data storage media once removed from ICT equipment, for example, physically drilling through the hard drives or electronic storage media; and
* securely wiping a disk or storage media using software.

Written confirmation that the data has been removed from the storage media must be obtained and retained by the Service Provider or Zoodata. Note that information that is no longer required must be reviewed by the data owner for any data retention requirements.

Mobile devices and computers

This section includes additional security considerations when using a Zoodata system-owned versus a privately-owned mobile device or computer.

#### Zoodata Owned Devices

To ensure the security of mobile devices and protection of Zoodata information, the following requirements must be met by mobile devices and computers issued by Zoodata:

* up-to-date virus protection, security software patches and software updates must be installed.
* protection of the information on the device with authentication control;
* installation of remote disabling, erasure or lockout software must be installed; and
* re-allocation, retirement or disposal of mobile devices in line with the section on Disposal of storage media.

Individuals are responsible for the security of the mobile devices at all times, including:

* ensuring the secure storage, backup, transmission, access and disposal of information contained on mobile devices;
* removing all information from the device when the device is disposed of, transferred to another person or is to undergo repair.;
* accepting full responsibility to comply with the Acceptable Use Policy, Occupational Safety and Health requirements and relevant law including the Road Traffic Code Regulation 265 (use of mobile phones by the driver of the vehicle); and
* ensuring they are not left in vehicles or in the office unattended. Individuals may be held liable for any negligence resulting in lost, stolen or damaged goods, or delay in reporting. Lost, stolen or damaged mobile devices must be reported to the relevant line manager as soon as possible. If stolen, a report should be made to WA Police to obtain an official report number for insurance purposes. For devices that are stolen and have remote disabling or erasure software installed, Zoodata may erase all data on the mobile device, including private data. Staff using the device for storing personal data do so at their own risk.

#### Privately Owned Devices

Staff are permitted to use privately-owned devices are permitted for work purposes, subject to the general conditions and requirements listed below.

* Individuals are responsible for payment of all costs incurred with the use of a privately-owned device, including the device itself, connection, usage and license costs (except where an industrial award has provisions for reimbursement of mobile telephone costs for employer initiated on-call or contact requirements). These costs include work related use.
* Should the device be mislaid, lost or stolen, staff might be instructed to wipe out the data on the device. This will include any private data held on the device.
* The user is responsible for the protection of Zoodata information (e.g. emails) stored on the private device at all times. This includes:
  + protecting the device with passcode control at a minimum;
  + removing all Zoodata information from the device when the device is disposed of, transferred to another person or is to undergo repair
  + secure transmission of data
  + ensuring current malware protection wherever possible;
  + installing auto-location technology to help locate lost or stolen devices;
  + appropriate security in accordance with this policy for any device used to back up or synchronise with the mobile device (i.e. backups to laptops must be encrypted and laptops also appropriately disposed etc.).

The above conditions and requirements under which the private devices may be used for work purposes may be altered without notice.

Where BYOD services are established and available for use, privately owned mobile devices may connect to the Zoodata network where the following are available and applied:

* the appropriate technical capabilities to support BYOD have been established for that site
* a Mobile Device Management Service exists or can be installed on the device to protect Zoodata system infrastructure and information. Such software may affect the performance of the device. Note that Zoodata is not responsible for any adverse impact of the software on the privately owned device.
* Zoodata Wi-Fi is available on site;
* an agreement has been signed by the requestor (user) indicating their acknowledgement of the conditions outlined at the above section on Privately Owned Devices and their compliance with the secure storage and transmission requirements outlined in the section on Data Storage, Transfer and Disposal.

### Remote Access of Zoodata Information via VPN

Zoodata provides remote access capabilities for flexible work arrangements and on call support over a VPN facility. This is available on request. Using the VPN allows Zoodata employees to access Zoodata information offsite without the need for the information to leave the organisation’s computer network.

### Network Security Management

To protect Zoodata’s confidential information and information related to business strategies and continuity, networks must be managed and controlled. Security mechanisms, service levels and management requirements of all network services are to be identified and included in network contract agreements. A “Defence in Depth” approach to Zoodata ICT access (such as network access control) is to be used where applicable, based on a risk assessment and cost/benefit analysis.

### Personnel Security

The requirements listed in this section must be addressed to ensure that staff members engaged by Zoodata are aware of their responsibilities in relation to information security and are suitable for the roles they are undertaking.

* Individuals and organisations providing services to the Zoodata who are not covered by confidentiality obligations under the Code of Conduct must be required to sign confidentiality agreements.
* All employees must complete mandatory training to understand their responsibilities in relation to Accountability, Ethical Behaviour, and Records Management.
* Service Providers and Zoodata must ensure staff are:
  + regularly educated on their information security roles and responsibilities at orientation and on an on-going basis as required
  + educated to recognise cyber and social engineering threats and the security responses required of them, including the reporting of incidents
  + made aware of the information security risks and threats in the use of social media, including that of identity theft, and
  + educated on the security incident management procedures and reporting of events.
* ICT operations support for Zoodata information systems that process information and service-desk support should be provided by personnel who are physically located in WA and subject to Australian and Western Australian laws and policies wherever possible. Some non-routine problem resolution, upgrade or maintenance services may be provided remotely by personnel located in jurisdictions external to Western Australia, however such services must be subject to strict security controls, network access under formal access arrangements and ongoing monitoring by staff members employed by a service provider or Zoodata.
* Exit checks for any individual completing their employment or contract with a Service Provider or Zoodata must include ensuring the individual has returned and accounted for all Zoodata information and ICT assets, including any security tokens and electronic records. This also includes equipment assigned to the individual for teleworking arrangements and all information held in a privately owned device. Personnel exit procedures must include the de-provisioning of any access that the person may have had to all Zoodata networks, infrastructure and applications. Individuals are to acknowledge they do not have possession of any Zoodata information.

### Physical Security

Physical and environmental security of ICT systems, infrastructure, facilities/buildings and network components is necessary to prevent unauthorised physical access, damage and interference to Zoodata information. Classified data may also require additional physical security requirements. A risk management approach should be followed to identify and implement physical and environmental security controls. This approach must consider the following:

* Physical security perimeter – protect areas that contain sensitive or critical information and ICT facilities (e.g. appropriate buildings structure of floor to ceiling walls, fire doors, intruder detection systems, CCTV).
* Physical entry controls – secure areas that only allow authorised personnel access (i.e. record of date/time of visitors, authentication mechanisms such as access cards, audit trail, visitors/personnel wear visible identification, third party granted restricted access).
* Secure offices, rooms and facilities – physical security of offices, rooms and facilities are incorporated in planning and building.
* Protecting against external and environmental threats – physical protection and avoidance against natural disasters, malicious attacks or accidents (i.e. planning decisions to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster).
* Working in secure areas – procedures for personnel and third-party providers on a ‘need to know’ basis, unsupervised work limited to avoid malicious activities, use of physical locks for vacant areas with review plans in place.
* Delivery and loading areas – control of access points for delivery and loading areas with isolation where possible to ICT processing facilities (i.e. restriction of personnel, secured external doors, inspection of incoming materials and recorded as per asset management requirements).
* Equipment position and protection – consideration of site and protection to reduce environmental threats and hazards or opportunities for unauthorised access (i.e. position of ICT facilities holding sensitive data to reduce viewing by unauthorised personnel, secure storage facilities, environmental controls such as humidity and temperate are monitored). Equipment should be correctly maintained to ensure its continued availability and integrity.
* Supporting utilities – ensure equipment from power failures and other disruptions by failures in supporting utilities is protected (emergency lighting and communications available, emergency switches/valves to cut off power, water, gas and other utilities located and working). Management is to be alerted in the event of an issue.
* Unattended equipment – ensure that equipment not in use is sufficiently protected (i.e. password protected screen saver on computers, log off applications not in use, security controls such as passwords on mobile devices).
* Clear desk and clear screen policy – sensitive or critical business information to be locked securely to prevent unauthorised viewing or reproduction of information, computers locked or logged off when unattended. Exceptions for workflow purposes to be approved by an Authorised Officer.
* Cabling security – power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.
* Off-site assets – equipment, information or software should not be taken off-site without prior authorisation. When off-site, security should be applied to off-site assets taking into account the different risks of working outside the organisation’s premises.

### Security Continuity

Information security continuity must be embedded in Zoodata business continuity and disaster recovery management processes to ensure the required level of security is maintained during an adverse situation. In order to achieve this, Zoodata as well as contracted agents must:

* establish a business ICT continuity plan, business ICT disaster recovery plan and an ICT incident response plan, consistent with the standards set in the Risk Management Guidelines. These plans need to detail procedures for managing cyber threats from the internet, social engineering and contain details of how staff should respond to cyber threats under various circumstances. The plan should also contain details for escalation to police, including contact details and who is authorised to file a police report.
* In accordance with the risk profile, regularly review, test and update plans to ensure they are contemporary and effective.

### Backup and Disaster Recovery

Zoodata’s disaster recovery plans must include documented backup plans and provision for redundancies where required to ensure ongoing availability of information processing facilities. Disaster recovery information must be classified sensitive and secured appropriately.

To prevent loss of data, backup copies of information, software and system images must be taken and tested regularly in accordance with the risk profile and agreed backup plan. Backups must be stored in a remote location and subject to regular testing to ensure they are reliable for use in an emergency.

Operational procedures must monitor the execution of backups and address failures of scheduled backups. For critical systems and services, backup arrangements must cover all systems information, applications and data necessary to recover the complete system in the event of a disaster and where appropriate backup data should be encrypted.

### Security Incident Management

An information security incident is any event that results in unauthorised access to data, applications, services, networks and/or devices, through bypassing underlying security mechanisms.

Security incidents may be accidental or intentional, and can include:

* access violations by an individual or software;
* breaches of information integrity or confidentiality;
* corruption or disclosure of health information;
* loss of availability of information systems;
* non-compliances with policies or guidelines
* breaches of physical security arrangements; and
* uncontrolled system changes.

Zoodata’s information systems and physical environments must be monitored for security incidents, which, if detected are then managed according to the incident response procedures (as relevant). In addition, the procedures listed below must be followed.

* For incidents relating to information systems maintained by external service providers, staff must report the event to the relevant ICT Service Desk. The Service Desk will record the incident in accordance with their Incident Management Procedure for reporting and escalation of events, and refer the incident to their ICT Security.
* Where a data breach has occurred, the organisational response must be managed in accordance with the Data Breach Response Policy.
* Where a major incident has occurred, personnel must refer to Disaster Recovery and Management Policy.

To prepare an effective response to ICT security incidents, any Service Provider information processing facility must ensure:

* an adequate management structure is identified and in place, with the appropriate authority and experience, to prepare, mitigate and respond to adverse situations;
* incident response staff have the necessary authority and competence to manage the incident and maintain required levels of security;
* documented plans, responses and recovery procedures, detailing how the Zoodata will manage and maintain its security to the predetermined level, are developed, approved, maintained and tested in accordance with the risk profile; and
* plans and procedures must be communicated to staff members to ensure all staff are aware of their security incident management procedures and reporting of events.

### Software Licensing, Installation, and Use

Only authorised and licenced software must be used at Zoodata as unauthorised software may introduce malware or viruses and to ensure security patching /updates are up to date. Usage must be in accordance with specified license or copyright terms and conditions. The acquisition, implementation, transfer and retirement of software, including the reassignment of existing site-specific applications from one site to another, must be in accordance this policy. The procurement of software licences must be in accordance with the Procurement and Contract Management Policy.

### System Acquisition, Development, and Maintenance

Information security requirements should be included as an integral part of the entire information systems development and maintenance lifecycle. This includes:

* integrating information security requirements in the early stages of requirements gathering and design for new information systems or enhancements to existing information systems;
* protecting information involved in application service transactions to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, message duplication or replay. Additionally, information passing over public networks should be protected from fraudulent activity, contract dispute, unauthorised disclosure and modification;
* adequately protecting system development, test and training environments, with consideration for the sensitivity of the data, access control, monitoring of changes to the environment and code stored therein, and the degree of outsourcing associated with the system development;
* testing security functionality during development. Test data should be selected carefully, protected and controlled;
* prohibiting the use of operational data containing personally identifiable or other confidential information for test purposes;
* implementing formal and structured change control processes to ensure adequate management of changes;
* separating development, testing and operational environments to reduce the risks of unauthorised access or changes to the operational environment;
* addressing information security objectives in project management phases and incorporating security risks in both operational and project risk assessments; and
* supporting required ICT infrastructure availability through measures such as redundancy, failover, fault tolerant approaches and capacity management

### Teleworking and Remote Access

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as telecommuting, flexible workplace, remote work and virtual work environments.

Requests for remote access are not automatic and some requests may be declined for reasons of security or infrastructure concerns.

The requirements listed below also apply.

* Appropriate infrastructure must be based on requirements
* Virus protection software must be installed and regularly updated.
* Security software patches must be applied where applicable
* The ICT infrastructure must be stored in a secure location.
* Zoodata workstations connected to the Zoodata network via dedicated links must not be connected to other networks or the internet by any means other than through the Zoodata network connection.
* Reasonable safeguards must be taken to protect equipment and data from theft, loss or damage at the off-worksite location.
* Data files must be regularly backed-up, preferably to corporate file servers, to avoid loss through equipment failure, damage or theft.

### Third Parties and Supplier Relationships

Where third party organisations are contracted to provide services that include ICT services for Zoodata, contracts must contain appropriate measures to ensure the protection of health information and infrastructure and adhere to system wide policy and processes. These measures include:

* criminal records screening of Contractors’ personnel
* due diligence and procurement operations
* an agreed and documented risk management approach to supplier process, product and function with a focus on the complete supply chain;
* provision for external audits and governance oversight that addresses privacy and security risks;
* documented agreements for network access by external parties in accordance with the information security requirements that ensure adequate security controls are in place as outlined in this Policy; and
* business documents to contain “Commercial in Confidence” wording within the footer template to protect Zoodata information/ intellectual property;

# Compliance, Monitoring, and Evaluation

Service Providers, Zoodata and Contracted agents of Zoodata must develop internal processes to manage and monitor compliance with this policy. The System Manager, may require certain systems and the Zoodata network to log transactions and communications whether private or business related. The System Manager may also carry out compliance audits to ascertain the level of compliance with this policy and may provide updates to Directors of ICT and other relevant persons regarding the findings of compliance monitoring activities.

Although systematic and ongoing surveillance of staff emails and internet access logs will not occur, Service Providers, Zoodata and the System Manager may monitor or investigate staff use of Zoodata ICT network systems and resources. This will only occur to confirm compliance with the requirements of this Policy and to investigate possible incidents of breaches of security, unauthorised access or Human Resources matters.

A breach in confidentiality and security may be subject to disciplinary action and other remedies available through legislative provision. Unauthorised access, use and disclosure of confidential data, staff misconduct, including breach of this Policy is misconduct pursuant to the Zoodata Code of Conduct and suspected cases may be investigated and actions decided on a case-by-case basis.

# Definitions

The following definitions are relevant to this policy:

1. **Authentication-** Verification that an entity is who/what it claims to be using a password, biometrics such as a fingerprint, or distinctive behavior such as a gesture pattern on a touchscreen.
2. **Authorisation-** Information that defines what operations an entity can perform in the context of a specific application.
3. **Confidentiality-** The treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be used or divulged to others in ways that are inconsistent with the understanding of the original disclosure, without permission.
4. **Cloud Computing-** Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
5. **Cloud Infrastructure-** Cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics.
6. **Data-** The term ‘data’ generally refers to unprocessed information, while the term ‘information’ refers to data that has been processed in such a way as to be meaningful to the person who receives it. In this policy the terms ‘data’ and ‘information’ have been used interchangeably and should be taken to mean both data and information
7. **Data Breach-** A data breach is an incident in which personal, confidential, sensitive or commercial information is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.
8. **Data Centre-** A data centre is a repository that houses computing facilities like servers, routers, switches and firewalls, as well as supporting components like backup equipment, fire suppression facilities and air conditioning. A data centre may be complex (dedicated building) or simple (an area or room that houses only a few servers).
9. **Data Custodian-** The person(s) responsible for the day-to-day management of a data collection, as nominated by the Data Steward. Data Custodians assist the Data Steward to protect the privacy, security and confidentiality of information within data collections. Data Custodians also aim to improve the accuracy, usability and accessibility of data within the data collection.
10. **Data At Rest-** Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network.
11. **Data In Transit-** Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. Data protection in transit is the protection of this data while it is travelling from network to network or being transferred from a local storage device to a cloud storage device. Effective data protection measures for in transit data are critical as data is often considered less secure while in motion.
12. **Data Integrity-** Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
13. **Defence in Depth-** Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. Components of defence in depth include antivirus software, firewalls, anti- spyware programs, hierarchical passwords, intrusion detection and biometric verification.
14. **Encryption-** Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorised users. This cryptographic method protects sensitive data by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key
15. **Information Security-** Practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
16. **Need to Know-** Under the Need-to-Know principle, users are only granted access to the information they need to perform their tasks
17. **Need to Use-** Under the Need-to-Use principle, users are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) they need to perform the task/job/role.
18. **Password-** A password is a secret word or string of characters used for authentication. This is the most commonly used mechanism of authentication. Many two factor authentication techniques rely on passwords as one factor of authentication.
19. **Personal Information-** Means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead - whose identity is apparent or can reasonably be ascertained from the information or opinion; or who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.
20. **Portable Device-** Portable devices include, but are not limited to: portable storage and removable media, and mobile phone and computing devices.
21. **Portable and Attractive Items-** items of plant and equipment considered to be high risk of theft or loss and warrant controls over their use and management. They are identified based on their associated relevant risk, including portability, attractiveness, security, and ease of theft or loss.
22. **Principle of Least Privilege-** Refers to the concept that all user accounts at all times should run with as few privileges as possible, and also launch applications with as few privileges as possible.
23. **Privileged User Accounts-** A user account that has the capability to alter or circumvent system security protections is known as privileged. It can also apply to users who may have only limited privileges, such as software developers, but who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications
24. **Privileges-** A privilege is an identified right that a particular user has to a particular system resource, such as a file folder, the use of certain commands, or an amount of storage.
25. **Provisioning-** Provisioning refers to the enterprise-wide configuration, deployment and management of multiple types of IT system resources. An organization's IT or HR department oversees the provisioning process, which is applied to monitor user and customer access rights and privacy while ensuring enterprise resource security.
26. **Roles-** Roles are groups of operations and/or other roles. Users are granted roles often related to a particular job or job function.
27. **Segregation of Duties or Separation Principle-** Segregation of Duties is an internal control designed to prevent error and fraud by ensuring that no single person can access, modify or use assets without authorisation or detection. The initiation of an event should be separated from its authorisation.
28. **Security Controls-** Safeguards or countermeasures to avoid, counteract or minimise security risks relating to personal property, or computer software.
29. **Single Sign On-** Single sign-on is an authentication process that allows a user to access multiple applications with one set of login credentials
30. **Staff Member-** A staff member of a service provider is an employee in the service provider, or a person engaged under a contract for services by the service provider. A staff member also includes an employee of Zoodata. AN agent of Zoodata is a person who is engaged under a contract for services by Zoodata.
31. **Two Factor Authentication-** Two-factor authentication requires the use of two of the three authentication factors. These factors are: Something the user knows (e.g., password, PIN, pattern); Something the user has (e.g., ATM card, smart card, mobile phone); and Something the user is (e.g., biometric characteristic, such as a fingerprint).