THE COVES

NATURALLY PERFECT

The Coves Information Management Policy

Table of Contents

1. Introduction

The Coves' intentions for publishing an Information Management Policy are not to impose restrictions that are contrary to The Coves' established culture of openness, trust, and integrity. Rather The Coves is committed to protecting The Coves' employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of The Coves. These systems are to be used for business purposes in serving the interests of the company, and of our clients in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee of The Coves who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable Information Management in all its forms at The Coves. These rules are in place to protect the employee and The Coves. Inappropriate use exposes The Coves to many different risks such as virus attacks, compromise of network systems and services, and legal consequences. The Information Management Policy ensures compliance to legislation such as POPI.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct The Coves' business or interact with internal networks and business systems, whether owned or leased by The Coves, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at The Coves are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with The Coves policies and standards, and South African laws and regulations. Exceptions to this policy are documented in section 5.2

4. Policy

4.1. General Use and Ownership of Electronic and Computing Devices

4.1.1. The Coves' proprietary information stored on electronic and computing devices whether owned or leased by The Coves, the employee or a third party, remains the sole property of The Coves.

4.1.2. The Coves' employees and operators have a responsibility to promptly report the theft, loss, or unauthorized disclosure of The Coves' proprietary information.

4.1.3. Employees use or share The Coves' proprietary information only to the extent it is authorized and necessary to fulfil your assigned duties.

4.1.4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use, and if there is any uncertainty, employees should consult their manager.

4.1.5. For security and network maintenance purposes, authorized individuals within The Coves may monitor equipment, systems, and network traffic at any time.

4.1.6. The Coves reserves the right to audit networks, devices, and systems on a periodic basis to ensure compliance with this policy.

4.2. Security and Proprietary Information

4.2.1. All mobile and computing devices that connect to The Coves' network must comply with this Policy.

4.2.2. System-level and employees level passwords must comply with the Password/Passphrase section of this document. Providing access to another individual, either deliberately or through failure to secure access to passwords, is prohibited.

4.2.3. Postings by employees from The Coves' email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of The Coves, unless posting is in the course of business duties.

4.2.4. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware and other threats such as phishing.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of The Coves authorized to engage in any activity that is illegal under South African law while utilizing The Coves' owned resources. The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.3.1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations. This includes but is not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by The Coves.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which The Coves or the end-employees does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting The Coves business, even if you have authorized access, is prohibited.
4. Introduction of malicious programs into The Coves network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using The Coves' computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or other legislation.
7. Making fraudulent offers of products, items, or services originating from The Coves' account.
8. Making statements about warranty, expressly or implied, unless it is a part of their regular duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

10. Port scanning or security scanning is expressly prohibited unless prior notification to The Coves' Information Officer is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal duties.
12. Circumventing employees' authentication or security of any host, network, or account.
13. Introducing honeypots, honeynets, or similar technology on The Coves' network.
14. Interfering with or denying service to any employees other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, an employee's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, The Coves employees to parties outside The Coves.

4.3.2. Email and Communication Activities

When using company resources to access and use the Internet, employees must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or other means, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within The Coves' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by The Coves or connected via The Coves' network.
7. Posting the same or similar non-business-related messages to any service.

4.3.3. Blogging and Social Media

1. Blogging by employees, whether using The Coves' property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of The Coves' systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate The Coves' policy, is not detrimental to The Coves' best interests, and does not interfere with an employee's regular work duties. Blogging from The Coves' systems is also subject to monitoring.
2. Employees are prohibited from revealing any of The Coves' confidential or proprietary information, trade secrets or any other material when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of The Coves and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

4. Employees may also not attribute personal statements, opinions or beliefs to The Coves when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of The Coves. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, The Coves' trademarks, logos and any other intellectual property of The Coves may also not be used in connection with any blogging activity.

4.4. Information Technology Equipment Disposal

Technology equipment often contains parts that cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In South Africa Act No. 59 of 2008: National Environmental Management: Waste Act, 2014 and Act No. 26 of 2014: National Environmental Management: Waste Amendment Act, 2014 both regulate what rules apply to the disposal of items that may be potentially harmful to the environment. In addition, hard drives, USB drives, CD and DVD-ROMs and other storage media contain various kinds of The Coves' data, some of which is governed by Act No. 4 of 2013: Protection of Personal Information (POPI) Act.

In order to meet the requirements of the POPI Act, all storage mediums must be properly erased or effectively destroyed before being disposed of. However, simply deleting or even formatting data storage mechanisms may not be considered sufficient. When deleting files or formatting a device, data is marked for deletion but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within The Coves including, but not limited to the following: personnel computers, servers, hard drives, laptops, mainframes, smartphones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), tablets, peripherals (i.e., keyboards, mice, speakers), printers, scanners, portable storage devices (i.e., USB drives), backup tapes, printed material.

4.5.1. Technology Equipment Disposal

- When Technology assets have reached the end of their useful life, they should be sent to the IT service provider's office for proper disposal.
- The IT service provider will securely erase all storage mediums in accordance with current industry best practices.
- All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting best practice standards.
- No computer or technology equipment may be sold to any individual other than through the processes identified in this policy.
- No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around The Coves. These can be used to dispose of equipment. The IT service provider will properly remove all data prior to the final disposal.
- All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program; this applies to all devices capable of being treated in this way. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

- Computer equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
- The IT service provider must place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

4.5.2. Employee Purchase of Disposed Equipment

- Equipment which is working but reached the end of its useful life to The Coves, will be made available for purchase by employees.
- Finance and Information Technology will determine an appropriate cost for each item.
- All purchases are final. No warranty or support will be provided with any equipment sold.
- Any equipment not in working order will be donated or disposed of according to current environmental guidelines.
- The Coves has contracted with several organizations to donate or properly dispose of outdated technology assets.
- Prior to leaving The Coves' premises, all equipment must be removed from the Information Technology inventory system.

4.5. Clean Desk

A clean desk policy is an important tool to ensure that all sensitive/confidential materials are removed from an end-user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information. This policy supports compliance with the POPI Act, Condition 7: Security safeguards, as well as the Information Security Standard ISO27001 and Quality Standard ISO9001.

The purpose of this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of sight. A clean desk policy is not only ISO 27001 compliant, but it is also part of standard basic privacy controls.

4.5.1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
4.5.2. Computer workstations must be locked when the workspace is unoccupied.
4.5.3. Computer workstations must be shut down completely at the end of the workday.
4.5.4. Any confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
4.5.5. File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.
4.5.6. Keys used for access to restricted or sensitive information must not be left at an unattended desk.
4.5.7. Laptops must be either locked with a locking cable or locked away in a drawer.

4.5.8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
4.5.9. Printouts containing restricted or sensitive information should be immediately removed from the printer.
4.5.10. Upon disposal, confidential documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
4.5.11. Whiteboards/glass boards containing confidential information should be erased.
4.5.12. Lock away portable computing devices such as laptops and tablets.
4.5.13. Treat mass storage devices such as CDROM, DVD or USB drives as a potential for risk of loss and secure them in a locked drawer.
4.5.14. Printing pin codes are used for the printing of confidential information.

The Coves management will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

4.6. Data Privacy

We collect and process personal information mainly to provide stakeholders with access to our estate and associated services, to help us improve our offerings and for certain other purposes which are outlined below.

4.6.1. Website and Social Media

The Coves does not collect or store any personal information through our website or social media platforms.

4.6.2. Visitors

The Coves Access Policy requires that personal information be obtained upon gaining access to The Coves.

Why we collect and store visitor's information?

The Coves collects and stores visitor information as per the Rules and Code of Conduct and the Security Protocol.

How will the information be stored?

The Coves will store the information electronically as per The Coves' Records Management Policy.

When will the information be deleted/destroyed?

The information relating to visitors will be deleted/destroyed after 30-days. Should an incident occur involving a visitor, the information of the said visitor will be retained until the matter has been finalised/closed.

4.6.3. Service Providers

As part of The Coves' Procurement Policy, service providers personal information will be obtained upon submission of a proposal to The Coves. This information will be processed and stored for a period of 5 years as per The Coves' Record Management Policy.

Why do we collect service providers information?

The Coves must as per the Procurement Policy store documents for a period of 5 years to prove that the procedure for obtaining proposals was followed.

Should a contract be awarded to a service provider, all information (proposals, invoices, contracts etc.) will be processed and stored for the period of the contractual agreement and thereafter be stored for 5 years from the termination of the agreement.

How will the information be stored?

The Coves will store the information electronically as per The Coves' Record Management Policy.

4.6.4. Contractors

In terms of the Architectural Guidelines, The Coves requires contractors to register before work may commence at a member's property.

Why do we require contractors to register with The Coves?

The Coves requires contractors to register to ensure that legislative requirements are met and to ensure that work being done at the property has been approved as per the Memorandum of Incorporation and Architectural Guidelines.

In terms of Builders Code of Conduct and Security Protocol it is also required that the contractor and its employees register for biometric access.

How will the information be stored?

The Coves will store the information linked to the property under the relevant property file and electronically as per The Coves' Records Management Policy.

When will the information be deleted/destroyed?

The information relating to the contractor will be deleted/destroyed once the project has been completed and the completion certificate has been issued by The Coves.

4.6.5. Members

Upon taking transfer of a property at The Coves, members are bound contractually by the Memorandum or Incorporation (MOI). Please refer to the MOI and Rules and Code of Conduct for more information on the processing of members personal information.

4.7. Information Backup

The Coves' information system resources are assets important to The Coves' business and stakeholders and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. It is The Coves' policy that appropriate backup measures are implemented to protect its information system resources from loss or corruption and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

Supporting standards, guidelines and procedures will be issued on an ongoing basis by The Coves. Users will be informed of any subsequent changes or updated versions of such standards, guidelines, and

procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from The Coves' service provider on an ongoing basis and accept the terms and conditions contained therein.

4.7.1. Build Documentation

The Coves' IT service provider will document and build processes and test recovery routines to mitigate risks of data loss.

4.7.2. Back-up Schedules

Back-ups are scheduled as one of the following:

- Monthly
- Annual
- Archive – Cloud drive
- As requested

According to standard definitions of terms, back-ups are determined as:

- Full
- Differential
- Incremental

Back-up logs will be reviewed daily by the IT service provider.

Should a backup failure occur, tests will be conducted to investigate the cause of backup failures and action taken accordingly to prevent a recurrence.

4.7.3. Restoration

- Test restorations will be conducted by the IT service provider at regular intervals using a disparate cross-section of application types to ensure that back-ups are working correctly and that restorations can be successfully executed.
- Where possible, restores are made initially to an alternate location, and then copied to the live location following verification.
- Where restoration is to a live system and the system is not terminally corrupt, the existence of a suitably-recent backup is confirmed in case the restoration fails. Where no suitably-recent backup exists, a backup is taken first.
- Users will be notified of the outcome of the restore.

4.7.4. Software Compatibility

A secure library of application software versions will be maintained for as long as corresponding backups are retained in order to ensure that a compatible version of the software will be available for use if the need arises to restore an application to a pre-upgrade state.

4.7.5. Back-up Retention

Back-ups are retained in accordance with the following periods of time:

Backup Schedule	Retention Period
Monthly	Minimum 3 months
Annual	6 years
Archive	Indefinite
Once-off	As requested

4.7.6. Media Storage

Back-ups are collected and stored offsite by an appropriately-resourced third party contractor. Footage held temporarily on site is stored in a controlled, secure environment.

4.7.7. Reporting Security Incidents

All security incidents, including significant backup or restoration failures, should be reported immediately to the Information Officer.

4.8. Disclosure of Personal Information

We may disclose Personal Information to our business partners who are involved in the delivery of products or services to our members, residents, and other relevant stakeholders. We have agreements in place to ensure that they comply with these privacy terms.

We may share your Personal Information with, and obtain information about you from:

- Other companies in our industry when we believe it will enhance the services and products, we can offer to you, but only where you have not objected to such sharing.

We may also disclose your information:

- Where we have a duty or a right to disclose in terms of law or industry codes.
- Where we believe it is necessary to protect our rights.

4.9. Personal Information Security

We are legally obliged to provide adequate protection for the Personal Information we hold and to stop unauthorised access and use of personal information. We will, on an on-going basis, continue to review our security controls and related processes to ensure that your Personal Information is secure.

Our security policies and procedures cover:

- Acceptable usage of personal information;
- Access to personal information;
- Computer and network security;
- Governance and regulatory issues;
- Investigating and reacting to security incidents.
- Monitoring access and usage of personal information;
- Physical security;
- Retention and disposal of information;
- Secure communications;
- Security in contracting out activities or functions;

When we contract with third parties, we impose appropriate security, privacy, and confidentiality obligations on them to ensure that Personal Information that we remain responsible for, is kept secure.

We will ensure that anyone to whom we pass Personal Information agrees to treat the information with the same level of protection as we are obliged to.

4.10. Accessing of Personal Information

Members, residents, visitors, service providers and contractors have the right to request a copy of the Personal Information we hold. To do this, simply contact us and specify what information you would like. We will take all reasonable steps to confirm the identity of the individual inquiring on the information before providing details.

Please note that any such access request may be subject to a payment of a legally allowable fee, as laid down in our PAIA Manual.

4.10.1. Correction of an individual's Personal Information

An individual has the right to request that we update, correct, or delete their personal information. We will take all reasonable steps to confirm the person's identity before making changes to the Personal Information we may hold. It is the responsibility of the member/service provider/contractor to take the necessary steps to keep their Personal Information accurate and up to date by notifying us of any changes we need to be aware of in writing.

4.10.2. Right to object

In terms of the POPI Act (POPIA) section 18. (h) (iv) you have the right to object to the processing of personal information as referred to in section 11(3) of the POPIA.

4.10.3. Right to lodge a complaint

In terms of the POPI Act (POPIA) section 18. (h) (v) you have the right to lodge a complaint to the Information Regulator (South Africa) (IRSA). The IRSA contact details are:

https://www.justice.gov.za/inforeg/contact.html
33 Hoofd Street
Forum III, 3rd Floor Braampark
P.O Box 31533
Braamfontein, Johannesburg, 2017
Mr Marks Thibela
Chief Executive Officer
Tel No. +27 (0) 10 023 5207, Cell No. +27 (0) 82 746 4173
Email inforeg@justice.gov.za

4.11. Data Security – Digital Devices

The following policies/rules have been adopted by The Coves and are required to be adhered to by staff using company devices:

4.11.1. The Coves has standardized on Apple iPhones because of increased security of data provided by IOS relative to Android-based devices, as well as better durability.
4.11.2. A 6-digit passcode must be enabled. This automatically ensures that the data on the iPhone is encrypted.
4.11.3. "Find my device" must be enabled. In the event of an iPhone being stolen or lost, it can be locked and/or erased.
4.11.4. Under settings, the Erase Data must be set to ON (under Face ID &Passcode). This will erase all data on the iPhone after 10 consecutive incorrect passcode attempts.

4.11.5. If the iPhone has been stolen or lost, the relevant AppleID must be deleted. This means that iPhones must be manually backed up to a company-owned device.
4.11.6. Two-factor authentication (2FA) must be used whenever available for secure logins.
4.11.7. All devices must always be updated with the latest operating software.
4.11.8. All devices must be rebooted (powered down) daily. Many malware products are susceptible to being deleted during reboot.
4.11.9. All computers and external drives are to be encrypted with Bitlocker which is standard in Windows 10.
4.11.10. Each Apple device must have the application firewall, Lockdown, installed in whitelist mode. The approved Android firewall is Netguard.
4.11.11. Only apps required for estate business are permitted to be installed on company-owned devices, and then, only from the Apple Appstore. No other apps are permitted.
4.11.12. Company-owned devices may only connect to the company Wi-Fi network. Exceptions to this rule must be approved by the company's Information Officer, by email with specific restrictions. Written permission from the Information Officer is required to permit the use of any public Wi-Fi facilities (airports, coffee shops, etc.).
4.11.13. All backups are to be encrypted. It is to be noted that iCloud and Google Drive do not support end-to-end encryption and should not be used for backups of data.
4.11.14. Security Passwords / Passphrases

In line with the Protection of Personal Information Act (POPIA), access to company laptops, PC's, cell phones and other electronic storage devices must be password protected.

In order to create secure passwords, passwords must be used that computers will take a long time to guess as modern computers can make somewhere between 10,000 and 350 billion guesses per second. To avoid a password being hacked and company information being compromised, making use of a passphrase is mandatory. Random passphrases provide the best combination of memorability and security. You can check the security of your password on sites like www.useapassphrase.com which is also useful for generating secure passphrases.

4.8.14.1 Passphrases should never be reused. This means that for each individual login, a unique passphrase must be created and used. A log of the unique login credentials should be maintained securely. A good way to do this is by using a password-protected spreadsheet. A digital password manager may be introduced in due course.
4.8.14.2 Each employee must ensure that access to electronic equipment provided by the company is protected by a secure passphrase.
4.8.14.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Please refer to You must lock the screen or log off when the device is unattended.

4.11.15. Website surfing must be conducted with extreme care and restraint. Many websites are set up primarily to collect data. (Remember that if you don't pay for the service, you are the product – at least the information on your device is).
4.11.16. Extreme care must be taken to ensure that mobile devices are safe from potential theft.
4.11.17. All external drives must be stored in a fireproof safe.
4.11.18. Anti-virus protection software must be installed and kept current.

4.12. Records Management

Records Management is important to ensure that all aspects of managing records support compliance with the POPI Act. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace.

This section supports compliance with the POPI Act, Condition 3: Purpose specification (section 14), Condition 5: Information Quality and Condition 7: Security safeguards, as well as ISO 15489-1:2001 Information and documentation – Records Management (Part 1 General) and ISO 15489-2:2001 Information and documentation – Records Management (Part 2: Guidelines).

The purpose is to establish the minimum requirements for records management in support of compliance with the POPI Act, good governance, and effective risk management. It:

- demonstrates to employees and stakeholders that managing records is important to the organization.
- provides a statement of intentions that underpins a records management program.
- serves as a mandate for the activities of the records manager.
- provides a framework for supporting documents such as procedures, business rules, disposal schedules etc.

This policy applies to all The Coves' employees and contractors.

- Format – it covers all records, whatever the technology used to create and store them and includes business systems as well as traditional correspondence files and email.
- Lifetime – it covers records throughout their life, from planning and creation through to disposal.
- Location – it includes records wherever they are and covers records managed on behalf of the organisation by external service providers (Operators).

4.9.1. Approved Storage Locations

- Filing cabinet (lockable)
- Back-up drives
- NAS Storage
- Data Cloud Server
- Cloud Storage Off-Site (3d Party)
- Document Storage Room (lockable)
- Document walk-in safe (lockable)
- Other (to be agreed)

4.9.2. Records Retention Periods

Records will be retained as per the records retention periods listed in the Records Management Policy.

4.9.3. Disposal of Records

Records will be disposed of after the retention period has expired and there is no further need to retain the record.

5. Policy Compliance

5.1. Compliance Measurement

The Coves' IT service provider will verify compliance to this policy through various methods, including but not limited to, ad hoc and periodic monitoring, internal and external audits, and provide feedback to the Information Officer.

5.2. Exceptions

Any exception to the policy must be approved by The Coves' Information Officer in advance.

5.3. Non-Compliance

An employee who becomes aware of any aspect of non-compliance with this policy, whether by themselves or another employee, whether accidental or through any other cause, must report this incident to The Coves' Information Officer.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Data Classification Policy
- Social Media Policy
- Minimum Access Policy
- Password Policy

Source and Definitions

The primary source of The Coves' Acceptable Use Policy (AUP) is SANS Institute (www.sans.org) and is based on their example AUP as at June 2014.

The definition of terms used in this policy can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

SA National Archives https://www.nationalarchives.gov.za/

Policy Templates provided by IACT