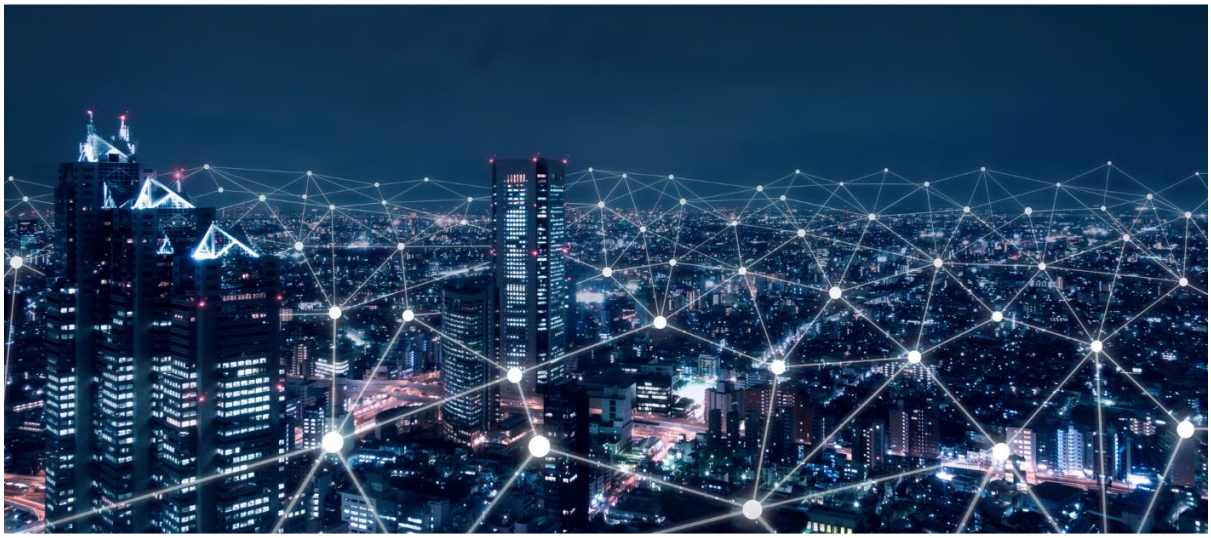
Block Secure

POPI POLICY



Antivirus and Malware Policy

1. Overview

The number of computer security incidents related to malware and viruses and the resulting cost of business disruption and service restoration continue to escalate. Implementing anti malware and antivirus systems, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are best practice actions that must be taken to reduce risks and manage the Block Secure (Pty) Ltd computing environment.

2. Purpose

The purpose of this policy is to describe requirements for preventing and addressing computer virus, worm, spyware, malware, and other types of malicious software.

3. Scope

This policy applies to all Block Secure (Pty) Ltd staff using Block Secure (Pty) Ltd information resources.

4. Policy

The Information Officer or their designee shall ensure:

- Procedures and tools exist to guard against, detect, and report malicious software
- IT personnel are trained and proficient in the use of the security solutions used to protect against malicious software
- End users are aware of the security policies enforced on their workstations

A. COMPUTING ASSETS

All workstation and server based assets used for business, whether connected to the Block Secure (Pty) Ltd network or as standalone units, must use Block Secure (Pty) Ltd approved antivirus/antimalware protection software and configuration provided by the Block Secure (Pty) Ltd The following procedures shall be followed:

- Virus protection software must not be disabled or bypassed
- Settings for the virus protection software must not be altered in a manner that will reduce the software effectiveness
- Automatic update frequency cannot be altered to reduce the frequency of updates
- All servers attached to the Block Secure (Pty) Ltd network must utilize Block Secure (Pty) Ltd approved/standard virus protection software and setup to detect and clean viruses
- All electronic mail gateways, devices, and servers must use Block Secure (Pty) Ltd approved e-mail virus/malware/spam protection software and must adhere to Block Secure (Pty) Ltd rules for the setup and use of this software

- Any threat that is not automatically cleaned, quarantined, and subsequently deleted by malware protection software constitutes a security incident and must be reported to The Information Officer

- Antivirus/antimalware signature updates shall occur on a frequency defined by the Block Secure (Pty) Ltd but shall occur minimally once each calendar day

B. APPLICATION INSTALLATION AND MANAGEMENT

All Block Secure (Pty) Ltd authorized applications and software shall be installed. Block Secure (Pty) Ltd managed antivirus and malware software shall ensure:

- Authorized applications and software operate according to a clearly defined security policy

- All unauthorized applications and software are prevented from being executed.

C. LICENSING, MAINTENANCE AND SUPPORT

Maintenance actions (software updates, definition updates, infections, etc.) shall be logged and retained for a period aligning with Block Secure (Pty) Ltd requirements to allow proper investigations into malware related incidents.

Management shall ensure proper licensing, tracking, and related documentation. This shall include processes and procedures supporting:

- Antivirus software installation on all systems

- Regular threat scanning capable of detecting, removing, and protecting against known types of malicious software

- Annual review and re-evaluation of low-risk systems and appliances not considered affected by malicious software based on current best practice

- Pro-active monitoring and update mechanisms supporting this policy

- Verification that mechanisms are in place for preventing users from disabling or modifying antivirus detection tools

- Processes and procedures for exceptions to the policy exist and are followed based on a case-by-case evaluation

- If antivirus mechanisms are disabled, additional security measures may need to be implemented for the period of time during which antivirus protection is not active.

5. Audit Controls and Management

On-demand documented procedures and evidence of practices should be in place for this operational policy. Appropriate controls include:

- Virus and malware installation and update logs

- Associated virus scan and history logs

- Procedures for quarantine and removal of threats
- Documented remediation and communication procedures for large scale incidents

6. VI. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

8. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Antivirus and Malware Policy	Yogis Naicker

Website Privacy Policy

1. Overview

Block Secure (Pty) Ltd ("us", "we", or "our") operates the Block Secure (Pty) Ltd website (the "Service").

This page informs you of our policies regarding the collection, use and disclosure of Personal Information when you use our Service.

We will not use or share your information with anyone except as described in this Privacy Policy.

We use your Personal Information for providing and improving the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions, accessible at http://blocksecure.co.za

2. INFORMATION COLLECTION AND USE

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information ("Personal Information") may include, but is not limited to:

- Name
- Email address
- Telephone number
- Address

3. LOG DATA

We collect information that your browser sends whenever you visit our Service ("Log Data"). This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages and other statistics.

4. COOKIES

Cookies are files with small amount of data, which may include an anonymous unique identifier. Cookies are sent to your browser from a web site and stored on your computer's hard drive.

We use "cookies" to collect information. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

5. SERVICE PROVIDERS

We may employ third party companies and individuals to facilitate our Service, to provide the Service on our behalf, to perform Service-related services or to assist us in analyzing how our Service is used.

These third parties have access to your Personal Information only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

6. SECURITY

The security of your Personal Information is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

7. LINKS TO OTHER SITES

Our Service may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over, and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

8. CHILDREN'S PRIVACY

Our Service does not address anyone under the age of 18 ("Children").

We do not knowingly collect personally identifiable information from children under 18. If you are a parent or guardian and you are aware that your child has provided us with Personal Information, please contact us. If we discover that a child under 18 has provided us with Personal Information, we will delete such information from our servers immediately.

9. COMPLIANCE WITH LAWS

We will disclose your Personal Information where required to do so by law or subpoena.

10. CHANGES TO THIS PRIVACY POLICY

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

11. CONTACT US

If you have questions or comments about this Cookie Policy, please contact us at:

010 065 1349
admin@blocksecure.co.za

12. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

13. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Website Privacy Policy	Yogis Naicker

Cookie Policy

1. Overview

Block Secure (Pty) Ltd (“we” or “us” or “our”) may use cookies, web beacons, tracking pixels and other tracking technologies when you visit our website including any other media form, media channel, mobile website, or mobile application related or connected thereto (collectively, the “Site”) to help customize the Site and improve your experience.

We reserve the right to make changes to this Cookie Policy at any time and for any reason. We will alert you about any changes by updating the Last Updated date of this Cookie Policy. Any changes or modifications will be effective immediately upon posting the updated Cookie Policy on the Site and you waive the right to receive specific notice of each such change or modification.

You are encouraged to periodically review this Cookie Policy to stay informed of updates. You will be deemed to have been made aware of, will be subject to and will be deemed to have accepted the changes in any revised Cookie Policy by your continued use of the Site after the date such revised Cookie Policy is posted.

2. Use of cookies

A “cookie” is a string of information which assigns you a unique identifier that we store on your computer. Your browser then provides that unique identifier to use each time you submit a query to the Site. We use cookies on the Site to, among other things, keep track of services you have used, record registration information, record your user preferences, keep you logged into the Site, facilitate purchase procedures, and track the pages you visit. Cookies help us understand how the Site is being used and improve your user experience.

3. Type of cookies

The following types of cookies may be used when you visit the Site:

4. Advertising Cookies

Advertising cookies are placed on your computer by advertisers and ad servers in order to display advertisements that are most likely to be of interest to you. These cookies allow advertisers and ad servers to gather information about your visits to the Site and other websites, alternate the ads sent to a specific computer, and track how often an ad has been viewed and by whom. These cookies are linked to a computer and do not gather any personal information about you.

5. Analytics Cookies

Analytics cookies monitor how users reached the Site, and how they interact with and move around once on the Site. These cookies let us know what features on the Site are working the best and what features on the Site can be improved.

6. Our Cookies

Our cookies are “first-party cookies”, and can be either permanent or temporary. These are necessary cookies, without which the Site won’t work properly or be able to provide certain features and functionalities. Some of these may be manually disabled in your browser, but may affect the functionality of the Site.

7. Personalization Cookies

Personalization cookies are used to recognize repeat visitors to the Site. We use these cookies to record your browsing history, the pages you have visited, and your settings and preferences each time you visit the Site.

8. Security Cookies

Security cookies help identify and prevent security risks. We use these cookies to authenticate users and protect user data from unauthorized parties.

9. Site Management Cookies

Site management cookies are used to maintain your identity or session on the Site so that you are not logged off unexpectedly, and any information you enter is retained from page to page. These cookies cannot be turned off individually, but you can disable all cookies in your browser.

10. Third-Party Cookies

Third-party cookies may be placed on your computer when you visit the Site by companies that run certain services we offer. These cookies allow the third parties to gather and track certain information about you. These cookies can be manually disabled in your browser.

11. Control of cookies

Most browsers are set to accept cookies by default. However, you can remove or reject cookies in your browser’s settings. Please be aware that such action could affect the availability and functionality of the Site.

For more information on how to control cookies, check your browser or device’s settings for how you can control or reject cookies, or visit the following links:

Apple Safari

Google Chrome

Microsoft Edge

Microsoft Internet Explorer

Mozilla Firefox

Opera

Android (Chrome)

Blackberry

Iphone or Ipad (Chrome)

Iphone or Ipad (Safari)

In addition, you may opt-out of some third-party cookies through the Network Advertising Initiative's Opt-Out Tool.

12. Other tracking technologies

In addition to cookies, we may use web beacons, pixel tags, and other tracking technologies on the Site to help customize the Site and improve your experience. A "web beacon" or "pixel tag" is tiny object or image embedded in a web page or email. They are used to track the number of users who have visited particular pages and viewed emails, and acquire other statistical data. They collect only a limited set of data, such as a cookie number, time and date of page or email view, and a description of the page or email on which they reside. Web beacons and pixel tags cannot be declined. However, you can limit their use by controlling the cookies that interact with them.

13. Privacy policy

For more information about how we use information collected by cookies and other tracking technologies, please refer to our Privacy Policy posted on the Site. This Cookie Policy is part of and is incorporated into our Privacy Policy. By using the Site, you agree to be bound by this Cookie Policy and our Privacy Policy.

14. Contact us

If you have questions or comments about this Cookie Policy, please contact us at:

010 065 1349
admin@blocksecure.co.za

15. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

16. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Cookie Policy	Yogis Naicker

Bring Your Own Device (BYOD) and Acceptable Use Policy

1. Purpose

The BYOD and Acceptable Use Policy are part of Block Secure (Pty) Ltd Security Program. Information security policies are the principles that direct managerial decision-making and facilitate secure business operations. A concise set of security policies enables Block Secure (Pty) Ltd to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorized behavior for personnel approved to use information assets, such as laptops, tablets and smartphones.

2. Applicability

The BYOD and Acceptable Use Policy applies to all employees, interns, contractors, vendors and anyone using assets. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by or its designated representatives.

3. BYOD POLICY

This policy provides guidelines for using personally owned devices and related software for corporate use.

4. Applicability

The BYOD policy applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the Information Officer or a designated representative.

Furthermore, based on the amount of personally identifiable information (PII) employees work with, management reserves the right to determine which employees can use personally owned devices and which cannot.

5. General Policy

recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely.

The following is a list of personally owned devices permitted by for corporate use:

- Desktop computers
- Laptop computers
- Tablets
- Personal digital assistants (PDAs)
- Smart phones
- Portable music players

6. Reimbursement

Block Secure (Pty) Ltd will NOT reimburse for the purchase of personally owned devices. Block Secure (Pty) Ltd is not responsible for any additional costs associated with learning, administering or installing these devices.

7. Registering Devices

All personally-owned devices must be registered with the Block Secure (Pty) Ltd.

8. End-User Support

As a general rule, users of personally owned devices will not use or request Block Secure (Pty) Ltd IT resources in the use, network connectivity or installation of their equipment or software. Users are responsible for learning, administering, installing and setting up their personally owned devices.

- Block Secure (Pty) Ltd will support personally owned devices as follows
- The user will be required to allow Block Secure (Pty) Ltd to load security software on each device.
- The user will be required to allow Block Secure (Pty) Ltd to install remote wiping software on each device.
- Upon request, the Block Secure (Pty) Ltd will install the necessary synchronization software to the user's desktop or notebook computer.

9. Device Security

The user should follow good security practices including:

- Password protect all personally owned devices
- Do not leave personally owned devices unattended

10. Release of Liability and Disclaimer to Users

hereby acknowledges that the use of personally owned devices in connection with business carries specific risks for which you, as the end user, assume full liability.

In the case of litigation, may take and confiscate a user's personally owned device at any time.

11. ACCEPTABLE USE POLICY

This policy provides rules for the acceptable use of personally owned devices on the corporate network.

12. Applicability

The Acceptable Use Policy applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the Information Officer or a designated representative.

13. General Policy

Users that wish to access the network using their personally owned computer may do so using only - authorized software and only with the approval of the Information Officer.

Users must follow the same rules when accessing the network from both corporate-issued equipment and personally owned devices. When connected to the network, the user will NOT:

- Use the service as part of violating the law
- Attempt to break the security of any computer network or user
- Attempt to send junk email or spam to anyone
- Attempt to send a massive amount of email to a specific person or system in order to flood their server

14. Authorization of Devices

Block Secure (Pty) Ltd the right to determine the level of network access for each personally owned device. The user could be granted full, partial or guest access.

15. Third-Party Applications on Devices

Block Secure (Pty) Ltd reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the company network.

As the number of approved applications continually evolves, the user must check with the Information Officer for the current list of approved third-party applications and get the Information Officer's approval before downloading it on the device.

16. Remote Wiping

While Block Secure (Pty) Ltd does not own the device, they do own all company data. Therefore, reserves the right to remotely wipe the user's personally owned device at any time. Not only will company data get wiped, but the user's personal data could be lost as well. The user must understand and accept this risk.

Furthermore, the user must agree to a full wipe of the personally owned device if they leave. This may result in the loss of both company and personal data on the device.

17. Reporting Security Concerns

The user agrees to report the following immediately:

- If the device is lost or stolen
- If the device has been attacked with malware, a virus or any other suspicious attack.
- Any other security concern with regards to company data

18. Release of Liability and Disclaimer to Users

hereby acknowledges that the use of a personally owned device on the network carries specific risks for which you, as the end user, assume full liability.

19. Bring Your Own Device (BYOD) and Acceptable Use Policy

Security of information, and the tools that create, store and distribute that information are vital to the long-term health of Block Secure (Pty) Ltd. It is for this reason we have established our BYOD and Acceptable Use Policy.

All employees are expected to understand and actively participate in this program encourages its employees to take a proactive approach in identifying potential problems or violations by promptly reporting them to their supervisor.

Prior to using personal devices for company purposes, each employee is expected to have read the entire BYOD and Acceptable Use Policy.

If you have any uncertainty regarding the content of these policies, you are required to consult your supervisor. This should be done prior to signing and agreeing to the BYOD and Acceptable Use Policy.

I have read and understand ’s BYOD and Acceptable Use Policy, and I understand the requirements and expectations of me as an employee.

20. VI. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

21. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

22. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	BOYD Policy	Yogis Naicker

Data Protection Policy

1. Overview

The Block Secure (Pty) Ltd is committed to processing data in accordance with its responsibilities under the Popi and Popia Act that requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

- This policy applies to all personal data processed by the Block Secure (Pty) Ltd.
- The Responsible Person shall take responsibility for the Block Secure (Pty) Ltd's ongoing compliance with this policy.
- This policy shall be reviewed at least annually.
- The Block Secure (Pty) Ltd shall register with the Information Registrar's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

- To ensure its processing of data is lawful, fair and transparent, the Block Secure (Pty) Ltd shall maintain a Register of Systems.
- The Register of Systems shall be reviewed at least annually.
- Individuals have the right to access their personal data and any such requests made to the Block Secure (Pty) Ltd shall be dealt with in a timely manner.

4. Lawful purposes

- All data processed by the Block Secure (Pty) Ltd must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
- The Block Secure (Pty) Ltd shall note the appropriate lawful basis in the Register of Systems.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Block Secure (Pty) Ltd's systems.

5. Data minimisation

- The Block Secure (Pty) Ltd shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

- The Block Secure (Pty) Ltd shall take reasonable steps to ensure personal data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

- To ensure that personal data is kept for no longer than necessary, the Block Secure (Pty) Ltd shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

- The Block Secure (Pty) Ltd shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted this should be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

- In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Block Secure (Pty) Ltd shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Information Registrar.

10. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

11. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Data Protection Policy	Yogis Naicker

Subject Access Request Policy

1. Overview

Under the Protection of Personal Information Act (POPI Act or POPIA) you, as a data subject, can ask us to confirm if we hold personal data about you; for copies of records of personal data that we hold, share or process about you; the period of time for which your personal data will be stored; the identity of any recipients of your personal data; the logic of automatic data processing, and the consequences of any profiling; and any other information relating to your personal data. This is known under the Popia as a data subject access request.

In order to deal with your request we can ask for proof of identity and enough information to enable us to locate the personal data that you request. Please complete this form and return it to us, or alternatively contact us in writing (post or email) to exercise your right to request the information described in this form, along with proof of your identity to:

Block Secure (Pty) Ltd
P O Box 53587
Troyeville
2139

admin@blocksecure.co.za

We will acknowledge safe receipt and we will respond to your request within one month of your request, where possible.

2. Part 1: Person that the request relates to (the data subject)

Title: Mr / Mrs / Miss / Ms / Other	
Surname:	
Forenames:	
Any other names that you are known by that may assist in the search:	
Address:	
Postcode:	
Telephone:	
E-mail:	

3. Part 2: Proof of identity

Please include a copy of your identity card or passport..

This is to ensure that we are only sending information to the data subject and not to a third party that has not been authorized by you. If none of these are available, please contact Block Secure admin@blocksecure.co.za for advice on other acceptable forms of identification.

4. Part 3: Information requested

To help us to deal with your request quickly and efficiently please provide as much detail as possible about the information you want.

I would like you to confirm if Block Secure (Pty) Ltd processes my personal data

☐	Provide a copy of my personal information
Provide supporting and explanatory material on the following as detailed below:	
☐	the purposes of processing
☐	the categories of my personal data processed
☐	the recipients, or categories of recipients of my personal data
☐	the envisaged retention period of my personal data, or, if this is not possible, the criteria used to determine this period
☐	my rights to rectification or deletion, to restrict processing or to object to processing, and to file a complaint to a data protection authority
☐	information regarding the source of the personal data (if you did not collect this from me)
☐	any automated decision making having legal or similar effects on me, as well as the logic involved and the consequences of the processing for me
☐	where my personal data are transferred abroad, the appropriate safeguards relating to the transfer
☐	I would like you to respond to my request and provide the information I have requested as follows:
☐	Email
☐	Post / Courier
☐	Collection

If possible, please restrict your request to a particular policy, service, department, team, individual or incident. Please include time frames, dates, names or types of documents, any file reference, and any other information that may enable us to locate your data. For example, for e-mails, please provide the names of senders and recipients, and approximate dates.

I,_____, confirm that the information provided on this form is correct and that I am the data subject whose name appears on this form. I understand that Block Secure (Pty) Ltd must confirm proof of identity and that it may be necessary to contact me again for further information to locate the personal data I want. I understand that my request will not be valid until all of the information requested is received by Block Secure (Pty) Ltd. I also understand that whilst this request is free of charge, if I request the same information again or make unfounded or excessive requests, Block Secure (Pty) Ltd may charge a reasonable administrative fee to process my request as per our Popi & Popia Manual.

Signature: _____ **Date**: _____

5. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

6. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Subject access request Policy	Yogis Naicker

Password Policy

1. Overview

The Password Policy defines the underlying requirements for management of strong user passwords to authenticate to system components within Block Secure (Pty) Ltd.

The scope of the Password Policy covers the whole of the business. This policy sets out when and why you need a password, how passwords can be created, used and changed.

2. Policy

1. It is Block Secure (Pty) Ltd policy to restrict access to systems and resources to legitimate users via means of a secure password.
2. The Block Secure (Pty) Ltd requirement for a password complexity of user accounts is as follows:
    a. Are required to have a password length of at least 8 characters;
    b. Are required to contain both alphabetic and numeric characters;
    c. Are required to contain at least one capital letter;
    d. Are required to contain at least one special character;
    e. Cannot use a password which is the same as any of the previous 4 passwords used;
3. Inactive user accounts will be disabled after no more than 90 days of inactivity, unless authorised by management where the retention of such accounts is required for operational purposes;
4. Password credentials:
    a. Should not be dictionary-based;
    b. Should not be shared with other user accounts on other systems;
    c. Should not contain any personally identifiable information (eg. names of family members or pets, dates of birth, etc.)
    d. Should not be shared with anybody for any reason;
    e. Should not be committed to hardcopy;
5. High-value/administrative accounts, such as accounts that allow the user to amend access rights and other important functionality, will require the use of multi-factor authentication (MFA) / two-step verification (2FA).

3. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

4. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Password Policy	Yogis Naicker

Personal Information Sharing Policy

1. Overview

It is sometimes necessary to share personal data or information with other Block Secure (Pty) Ltd staff or with other organisations with which we have a relationship to ensure effective coordination and integration of services for our clients.

This guidance details the requirements for sharing personal data in a safe and appropriate way in adherence with the Data Protection Act 1998.

As a data controller we notify the Information Commissioner's Office on an annual basis about the way in which we process personal information and we also provide examples of the types of sharing that is commonly undertaken.

Sharing information refers to the disclosure of information internally between different parts of the Block Secure (Pty) Ltd or externally to a third party organisation.

2. Collecting personal data

The consent of the data subject should be obtained for collecting their personal data. Consent should be "informed" and "unambiguous". This means that the data subject needs to be told what information is to be shared, who it will be shared with, and why. They should be given the opportunity to object to the sharing of the data, or told that they can withdraw their consent at a later date. If consent is refused at any stage, a record should be kept of refusals, with dates. Explicit consent needs to be sought for the collection and processing of sensitive data.

It is acceptable to share information on a 'need to know' basis within the Block Secure (Pty) Ltd where client information is required for someone to do their job. However, sensitive personal data (e.g. disability or health information) should not normally be shared without the explicit consent of the client – this means individuals must be fully aware of who the information will be shared with and should have given their agreement to this.

3. Reason or purpose for sharing data

Sharing personal data is not an automatic assumption and you must have a clear purpose for doing so e.g. achieving an objective that can only be achieved by sharing the information.

Personal data can only be shared if there is a clear legal basis to do so or if the data subject has given their clear consent.

If you are required to share personal data you should be clear about the reasons for sharing the data, and what you intend to achieve by doing so. Ask yourself if the sharing of a particular piece of data is necessary for the working relationship.

When you collect any personal data you should always document the purpose you have for collecting the data, how it will be used, and with whom it will be shared. This should be reviewed and updated on a regular basis. Where databases of information are shared, responsibilities of staff should be made clear. Senior managers need to ensure compliance on their particular areas.

Any third party organisations with which you share information should separately, as data controllers, notify their purposes for processing data to the Information Commissioner. It may be that the different parties process or use shared information for the same purposes. Or it may be that the parties have different purposes for processing or using information. If the purposes differ, each party must ensure that they are separately abiding by the principles of the Data Protection Act, and that they are specifying their purposes to the Information Commissioner. Using information for different purposes can be acceptable, as long as it is compatible with, or "not contradictory" to the original purpose for collection of personal data.

There is a "research" exemption of the Data Protection Act that does allow for the further processing of personal data, as long as it is only for research purposes (including statistical or historical purposes), and as long as the data is not processed to support measures or decisions about individuals; and is not processed in such a way that substantial damage or distress is likely to be caused to the individual.

4. Data Protection principles

There are eight data protection principles that must be adhered to in all cases when sharing any information:

Principle One

Personal data shall be processed fairly and lawfully and, shall not be processed unless: -

a) at least one of the conditions in Schedule 2 (of the Act) is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 (of the Act) is also met.

Individuals should be made aware of which organisations are sharing their personal data and what their data is being used for.

Principle two

Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

Principle three

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle four

Personal data shall be accurate and, where necessary, kept up to date.

Principle five

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle six

Personal data shall be processed in accordance with the rights of data subjects under the Act.

Principle seven

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

5. Disclosure of personal information

When disclosing personal data to a third party you should, where practicable, keep a record of the date and details of the transfer of information.

6. Respect for confidentiality of data subjects

The law of confidence is a common law concept, which means that there is no Act setting it out, but that it has been developed by the courts over individual cases. A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. Examples may include safeguarding issues, health and wellbeing (including mental health), reporting of incidents and personal issues/circumstances. The duty of confidentiality applies whether the information has been requested or volunteered.

Data subjects sometimes allow us to gather sensitive information relating to their personal circumstances, health and wellbeing. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately.

Members of staff will often receive information of a personal and sensitive nature ranging from information required for administrative purposes related to application and enrolment to more sensitive information shared with tutors or wellbeing services. Compliance with confidentiality is the responsibility of all staff of Block Secure (Pty) Ltd. Breaching confidentiality inappropriately could lead to legal action and loss of reputation.

Respecting confidentiality is essential. Without the trust that confidentiality brings, data subjects might not seek help and advice, or they might not give all the facts needed to provide for their education, health and wellbeing.

Staff must ensure that personal information is not disclosed to unauthorised third parties which includes family members, friends, Government bodies and in certain circumstances, the police. All staff should exercise caution when asked to disclose personal information held on a data subject to a third party.

Personal information is usually disclosed with the consent of the data subject. When using, sharing or disclosing information you should:

- inform the person about possible uses of their information

- ask for consent before disclosing information that could identify them, if the information is needed for any other purpose
- disclose information that identifies the person only if this is necessary to achieve the purpose of the disclosure – in all other cases information should be anonymised before disclosing it
- keep disclosures to the minimum necessary and on a strictly 'need to know' basis

Sharing information with the right people can help to protect individuals from harm and ensure that they get the help they need. It can also reduce the number of times they are asked the same questions by different people.

If data subjects are able to take part in decision-making, you should explain why they need to share information, and ask for their consent. By asking for their consent to share relevant information, you are showing respect and involving them in decisions about their education, health and wellbeing.

7. Sharing information without consent

There are certain circumstances when a data subject might not agree to disclosure but you still need to disclose information e.g.

- when there is an overriding public interest in the disclosure
- when it is judged that the disclosure is in the best interests of a student who does not have the maturity or understanding to make a decision a disclosure
- when disclosure is required by law
- when the data subject is at risk of sexual, physical or emotional abuse
- when the information would help in the prevention, detection or prosecution of serious crime
- when the data subject is involved in behaviour that might put them or others at risk of serious harm

8. Sharing information with the police

There is an exemption under the Data Protection Act which allows us to disclose information to the Police. This is known as the 'Section 29' exemption and covers disclosure for 'the prevention or detection of crime' and 'apprehension or prosecution of offenders'.

The police do occasionally ask for personal data as part of an inquiry but they don't have the automatic right to receive information about our staff or clients. You should not be pressured into handing over personal information. There is a special process to allow the police to access personal data for certain crime-related purposes. Please contact the Information Officer for further advice.

9. Consent

- Consent under POPI has to be specific, voluntary and informed.
- Since the burden of proof would be on you to show that it was given, some sort of record would be desirable.
- It's also important to remember that under 18s normally need a competent person to give consent.

Section 14(2) – (7) have further exceptions relating to retention for research / statistical purposes, where the personal information was used in a decision about the data subject, restriction of records etc.

It will probably be difficult to achieve a retention policy that covers the potentially thousands of record categories used by the organisation. One strategy is to start with the most widespread documents, like invoices and / or those containing the most sensitive personal information.

10. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

11. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Personal Information Sharing Policy	Yogis Naicker

Security Compromise Policy

1. Overview

Block Secure (Pty) Ltd has implemented the following procedures to follow in the event of a data security breach involving personally information or other confidential information maintained on personal computers, Block Secure (Pty) Ltd networks, or internet programs used by staff and consultants.

The following staff have key responsibility for implementing and executing the data breach procedures:

- Seelan Naicker (011 474 4657, 082 800 1036)

2. Procedure

In the event of a data breach or imminent breach of data, in order to contain the data breach and minimize the extent of the intrusion:

- Disconnect the affected and related systems or networks from Internet access.
- Contact the information officer to notify them of the data breach or imminent breach of data.
- Document date and time the breach occurred, what files the user was accessing at the time of the breach, the breach team member contacted, and actions taken to secure data.
- Contact technical support to detect and remove the malware or other information related to the breach.
- Review virus/malware/other protective software to review system vulnerabilities and increase the level of protection for the system.
- If possible, reimage the system and restore from backup files.

3. Mitigation

Following the incident, Block Secure (Pty) Ltd staff will review procedures to determine if any actions by the user or the team contributed to the data breach. Staff will be updated on policies to protect against data breaches or imminent breaches of personal data.

A computer technician will review software, updates, and software/data protection programs to improve the security of the data and operating system to prevent further incidents. Information related to the data breach will be documented on the incident log, repairs or modifications implemented will be included on the log and kept in a secure location.

If necessary, the management team will review procedures and make necessary changes to the procedures to improve the security of personal and other secure information.

4. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

5. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Security Compromise Policy	Yogis Naicker

Data Retention Policy

1. Overview

POPI requires that 'records of personal information must not be kept any longer than is necessary for achieving the purpose for which the information was collected…" Section 14(1) Practically this may be one of the most difficult provisions to comply with as it requires a very clear picture of all purposes for which a piece of information is kept and a thorough understanding of business processes. There are some exceptions to this rule, where the information may be kept for longer.

2. When required by law

- Records may be retained for longer when the retention "is required or authorised by law" Section 14(1)(a)
- Since numerous laws mandate the retention of different categories of record it can be a challenge just to find the relevant law.
- This guide detailing retention periods listed below

3. Required by contract

- As an example, your service contract with a customer might state that you are required to provide your customer with important safety updates regarding your product. In order to perform under the contract you would therefore need their contact information.

4. Consent

  - Consent under POPI has to be specific, voluntary and informed.
  - Since the burden of proof would be on you to show that it was given, some sort of record would be desirable.
  - It's also important to remember that under 18s normally need a competent person to give consent.

Section 14(2) – (7) have further exceptions relating to retention for research / statistical purposes, where the personal information was used in a decision about the data subject, restriction of records etc.

It will probably be difficult to achieve a retention policy that covers the potentially thousands of record categories used by the organisation. One strategy is to start with the most widespread documents, like invoices and / or those containing the most sensitive personal information.

5. ACCOUNTABILITY

Document	**Period of Retention**	
Accounting Records	**Retention in years**	**Reference**
Ancillary books of account and supporting schedules	15	2&4
Annual financial statements	15	2&4
Annual financial statements working papers	4	4
Bank instructions	4	4
Bank statements and vouchers	4	4
Bills of exchange	6	10
Books of account	15	2&4
Cash books	15	2&4
Cheques	4	13
Consolidation schedules	15	2&4
Costing records	5	2
Creditors' invoices and statements	5	2
Creditors' ledgers	15	2&4

Debtors' ledgers	15	2&4
Debtors' statements	4	4
Deposit slips	4	4
Dividend and interest payment lists (listed company)	15	2
Fixed asset register	15	2&4
General ledgers	15	2&4
Goods received notes	4	4
Insolvent businesses	3	12
Payrolls	7	4&7
Petty cash books	15	2&4
Purchases invoices (with supporting documentation)	4	4
Purchase journals (with supporting documentation)	15	2&4
Purchase Orders	4	4
Railage and shipping documents	4	4
Receipts	4	4
Sales invoices (with supporting documentation)	4	4

Sales journals	15	2&4
Second hand goodsDetails of acquisition and disposal	3	19
Shipping documents – inwards and outwards(after completion of shipment date)	2	5
Stock records (supporting schedules)	15	2&4
Stock sheets	4	4
Year end working papers for companies	4	4
Document	**Period of retention**	
Contracts and Agreements	**Retention in years**	**Reference**
Agreements of historical significance	Permanently	n/a
Debts (The Prescription Act should be referred to as the period depends on the type of debts)	4-30	4&10
Indemnities and guarantees (after date of expiry)	5	1
Licensing agreements (after date of expiry)	5	1
Rental and hire purchase agreements, suspended sale agreements (after date of expiry)		1

Document	**Period of retention**	
Correspondence	**Retention in years**	**Reference**
General	3	1
Accounting related	5	1
Agreements (after termination)	5	1

Document	**Period of retention**	
Employee Records	**Retention in years**	**Reference**
Accident books and records	7	6&7
Application for jobs – unsuccessful	1	1
Apprentice records of remuneration	3	6
Arbitration award records	3	15
Collective agreement records	3	15
Determination records made in respect of Wage Act	3	6&15

Dispute records prescribed details of any: • Strike • Lockout • Protest action involving employees	3	15
Expense accounts	4	4
Factory register	Permanently	8
Payrolls	7	4,6&7
Personal records of organisation's executives (for historical purposes)	Permanently	n/a
Salary revision schedules	7	6&7
Salary wage register	7	7&4
Staff records (after date employment ceases)	7	6&7
Tax returns – employees	4	4
Time and piecework records	7	6&7
Unemployment insurance contributor's card	Until service terminated	6
Wage and salary records (including overtime details)	7	4,6&7
Workmen's Compensation documents	3	
		

Document	Period of retention	
Insurance	**Retention in years**	**Reference**
Claim reports and accidents reports (after date of settlement)	3	1
Policies (after date of lapse)	4	4

Document	Period of retention	
Investment Records	**Retention in years**	**Reference**
Certificates and other documents of title	Permanently or until sold	n/a
Schedules and documents (after date investment sold)	15	2&4
Share investment certificates	Permanently or until sold	n/a
Transfer of marketable securities	5	2&4

Document	Period of retention	
Patents	**Retention in years**	**Reference**
Patent agreement with staff	Duration of patent or service of employee	1

Report and opinion on patents and trademarks (after date of expiry)	5	1

Document	**Period of retention**	
Pension Records	**Retention in years**	**Reference**
Actuarial valuation reports	10	1
Contribution records	4	4
Fund's annual account	Permanently	n/a
Group health, life and personal accident policies (after date of final cessation of any benefit payable under the policy)	5	1
Individual life policies under "Top Hat" schemes (after date of final cessation of benefit)	5	1
Investment records	15	2
Minutes of meetings of members and trustees	Permanently	n/a
Pension fund account records	15	2
Pension fund rules (including superseded rules)	Permanently	n/a

Document	**Period of retention**

Property Records	Retention in years	Reference
Agreements with architects and builders (after date of completion)	5	1
Deeds of title	Permanently or until dispoded	n/a
Leases (after date of expiry of lease and all queries have been settled)	5	2&4
Sectional title records	Permanently	n/a
Transfer duty records	Permanently	n/a

Document	Period of retention	
Share Registration Records	**Retention in years**	**Reference**
Acceptance forms	12	1
Accounting records of stock of brokers and carrier against shares	5	18
Allotment letters	12	1
Allotment sheets and return of allotment	15	2
Annual return and supporting documents	15	2
Application forms	12	1

Cancelled share of debenture certificates and balance receipts (many large transfer offices keep for one year only)	3	1
Cancelled share transfer forms	12	1&3
Change of address – notification	1	1
Dividends and interest • mandates (from date of receipt) • paid warrants • payment lists • unclaimed	 3 12 15 until cleared	 1 1 1
Letters of indemnity for lost share certificates	Permanently	1
Power of attorney, stop notices and similar court orders (from date person ceased to be a member)	15	1
Redemption / conversion discharge forms of endorsed certificates	12	1

Document	**Period of retention**	
Statutory Records	**Retention in years**	**Reference**
Combuned company register including:		
• Branch register	15	2

• Index of members	15	2
• Register of debenture holders	15	2
• Register of directors' attendance	15	2
• Register of directors and officers	15	2
• Register of directors' interest on contracts	15	2
• Register of members	15	2
• Register of pledges and mortgages	15	2
Documents of incorporation including:		
• Certificate of change of name	Permanently	2
• Certificate of incorporation	Permanently	2
• Certificate to commence business	Permanently	2
• Founding statement and amendments (Close Corporations)	Permanently	2&11
Memorandum and Articles of Association	Permanently	2
Minutes of meetings (originals for:		
• Board meetings	Permanently	2
• Committee meetings	Permanently	2

• General meetings	Permanently	2
• Minute books	Permanently	2&11
• Notification of change of address	1	1
Notices of general and class meetings proxy forms:		
• used	3	2
• used at court convened meetings	3	2
Special resolutions / resolutions passed at general / class meetings		
class meetings	Permanently	2
CM25	Permanently	2
CM26	Permanently	2
▲		
Document	**Period of retention**	
Tax Records	**Retention in years**	**Reference**
Income tax required records	4	4
Taxation returns and assessmentsRecords of subscriptions or levies paid by its members	15	12

Document	Period of retention	
VAT Documentation	**Retention in years**	**Reference**
Bank statements, deposit slips, stock lists paid by its member	Four years from last date of entry	13
Books of accounts	Four years from last date of entry	13
Detailed records of the registered vendor's transactions	4	13
Invoices, tax invoices, credit and debit notes	Four years from last date of entry	13
System documentation		
Charts and codes of accounts	4	13
Accounting system instruction manuals	4	13
System and program documentation	4	13
Other	4	13
In the case of all other records that are not required for the submission of the income tax return, for a period of 5 years from the date of the last entry in any book, or, if not in book form, from date of completion of the transactions, acts or operations to which they relate.		

6. Reference

1. Standard practice.
2. Companies Act No.61 of 1973 - Regulations for the Retention and reservation of Records (R2592 of 25 November 1983).
3. Stamp Duties Act No.77 of 1968, Section 23(6).
4. Income Tax Act No.58 of 1962, Sections 75(1) and (2).

   In terms of the Income Tax Act No. 58 of 1962, Section 75 “The Commissioner may, subject to such conditions as he may determine, and in respect of such books (other than ledgers, cash books and journals) or documents as he may specify, authorize the retention of any book or document referred to in subsection (1) in a form acceptable to him lieu of the original thereof."

   For years of assessment ending on or after 1 January 1993, all accounting records are to be retained for a period of five years from the date of receipt by Revenue, of the tax return, which incorporates information drawn from the last entry of that record.

   The Income Tax Act No.113 of 1993 changed the retention period from five years to four years for years of assessment ending on or after 1 January 1994. The Taxation Laws Amendment Act No.97 of 1993 brings the retention period for VAT documents into line with the requirements of the Income Tax Act No.113 of 1993.

   Consequently, the retention of accounting records for the 1993-year of assessment is five years from the date of receipt by Revenue of the tax return which incorporates information drawn from the last entry of the that record. For years of assessment ended on or after 1 January 1994 the period at retention has been reduced to four years on the same basis as for the 1993-year of assessment.

5. Customs and Excise Act No.91 of 1964, Section 101 and Regulation 1.04- Government Gazette No 4040 R17770 dated 5 October 1973.
6. Basic Conditions of Employment Act No.75 of the 1997, Section 29(4), 31(2). Manpower Training Act No.56 of 1981, Section 44(3). Unemployment Insurance Act No.30 of 1966, Section 32(1). Wages Act No.5 of 1957, Section 29(3).
7. Compensation for Occupational Injuries and Diseases Act, No.130 of 1993 Section 81(2). (Departmental practice recommends a limit of seven years on the requirement to preserve records).
8. Occupational Health and Safety Act No.85 of 1993 Section 8(1).
9. Co-Operatives Act No.91 of 1981 Section 237.
10. Prescription Act No.68 of 1969, Section 11c. The effect of prescription is, that the rights resulting from a contract are no longer enforceable by direct legal action:

    • But the rights themselves are not destroyed, because the corresponding obligation or debt remains as a natural obligation;

    • Therefore for safety reasons, documents should be kept longer than the periods laid down in the Prescription Act;

    • Moreover, these periods can be extended because of interruption or suspension of the prescription.

11. Close Corporations Act No.69 of 1984, Regulations.

12. Insolvency Act No.24 of 1936, Section 155 and Section 134 (1).
13. Value Added Tax Act No.89 of 1991, Section 55 (1)
14. Guidance and Placement Act 62 of 1981, Section 15 (5).
15. Labour Relations Act No.66 of 1995, Section 53 (4), 54(1),98(4), 99; 205 (2)(a).
16. Transfer Duty Act No.40 of 1949 Section 15(1).
17. Mutual Banks Act No.124 of 1993, Section 42.
18. Stock Exchange Control Act No.1 of 1985, Section 43.
19. Second Hand Goods Act No. 23 of 1955 Section 6(8).
20. Sale and Service Matters Act No. 25 of 1964, Section 11.
21. Electronic Communication and Transactions Act, 25 of 2002.
22. Promotion of Access to Information Act, 2 of 2002
23. Promotion of Administration Justice Act, 3 of 2000
24. National Archives and Record Services Act, 43 of 1996 (as amended)
25. Public Finance Management Act, 1 of 1999
26. Financial Intelligence Centre Act, 38 of 2001
27. STANSA 15489, South African Standard for Record Management.
28. Green paper on e-Government.

7. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

8. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Data Retention Policy	Yogis Naicker

CCTV Policy

1. Overview

Block Secure (Pty) Ltd operates closed-circuit television (“CCTV”) surveillance infrastructure on its premises.
The cameras are positioned so that they record arears. Footage of these areas is recorded and stored for a limited amount of time.

Block Secure (Pty) Ltd undertakes to ensure that its employees adhere to the strictest levels of confidentiality and respect individual’s right of privacy.

2. ACCOUNTABILITY

Block Secure (Pty) Ltd "processes" "Personal Information" (which contained in the CCTV surveillance footage) as contemplated in the Protection of Personal Information Act, No. 4 of 2013 (the “Act”), at all times taking into account individual’s constitutional right to privacy.

The authorisation for the collection, location and access of the CCTV surveillance footage ("Data") lies with Block Secure (Pty) Ltd. The Data may then be accessed, through Block Secure (Pty) Ltd’s systems, with the Information Officer’s express prior written consent..

Block Secure (Pty) Ltd shall fully comply with its obligations in terms of the Act, depending on the capacity in which it is acting any given circumstance.

Block Secure (Pty) Ltd will be processing Personal Information where, given the purpose for which it is processed, such processing is adequate, relevant and not excessive.

Details and records of all information processed by Block Secure (Pty) Ltd will be maintained to the extent required by law.

3. Purpose

The purpose of this policy is to outline Block Secure (Pty) Ltd's approach to the use of CCTV surveillance for purposes in line with the Act. Specifically, the Block Secure (Pty) Ltd strives to:

- process any Data lawfully, and in reasonable manner which does not unreasonably infringe on the privacy of the data subject;
- only process Data where, to do so, protects a legitimate interest of members of the public;
- ensure each individual's constitutional right to privacy, by safeguarding Personal Information when processed by it or any of its customers (each of which constitutes a Responsible Party in terms of the Act), subject to justifiable limitations;
- balance the privacy rights of individuals against other rights, particularly the rights of employees and customers to safety and security;
- regulate the manner in which Data may be processed, by establishing conditions in accordance with locally applicable laws and international standards, that prescribe the minimum threshold requirements for the lawful processing of Personal Information;
- advise individuals of their rights and remedies in order to protect their Personal Information from processing that is not in accordance with the Act; and
- comply with voluntary and compulsory measures, including those established by the Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by the Act.

The purpose of Block Secure (Pty) Ltd CCTV surveillance network is to:

- detect, deter and prevent crime;
- enhance safety of those who work and visit the areas covered by the CCTV surveillance network;
- assist in the apprehension and prosecution of offenders of crime (including but not limited to the use of images and video as evidence in criminal/civil proceedings
- Data gathered by the CCTV surveillance network will not be used for any purposes other than those listed above and/or permitted by the Act.
- Data will not, under any circumstances, be released to the media or any similar outlet, nor will any Data be released or disseminated unless specifically required or authorised by law.

- All Data will be stored on hosted servers and identified using an automatic recording sequence. The Data will be stored for a period of at least 30 days, being the length of time the Data is required to be maintained in order to achieve the purpose for which it was collected.
- This retention period may be increased or decreased in line with any lawful instruction provided by the Information Regulator or other competent authority from time to time. Data may be stored for a longer period should it be required for further investigation.
- At the expiry of this retention period, the data will be permanently deleted and/or destroyed in accordance with POPIA stipulated guidelines.
- No cameras will be hidden or obscured, nor will they be placed in such a fashion that any camera will be able to record activity in any area which is not considered to be 'public'
- All captions inserted onto collected Data, such as camera location, time and date, are securely maintained and stored and are incapable of being tampered with.

4. PUBLIC AWARENESS OF CCTV SURVEILLANCE

- Prior to the deployment of CCTV cameras, Block Secure (Pty) Ltd, together with stakeholders make its intention know to commence CCTV surveillance in that area.
- In order to ensure that all members of the public entering any area in which the CCTV surveillance network operates are informed of the surveillance, prominent signs will be posted in these areas.

5. Policy

1. It is the responsibility of all employees and agents to:
    a. Ensure the security and confidentiality of personal information.
    b. Protect against anticipated threats to the security and/or integrity of such information.
    c. Guard against unauthorised access to or use of such records or information that could result in substantial harm or inconvenience to any data subject.
2. The reasons for shredding documents are:
    a. To ensure that personal information is safeguarded and not accessed by unauthorised individuals; and
    b. To encourage the efficient recycling of all printed materials.
3. If using off site shredding services, all shredding containers should be locked whilst awaiting emptying or collection. Documents to be shredded should be place in the appropriate container and should not be left to accumulate in offices. Only reputable shredding service providers shall be used.
4. For offices that shred their own documents, the shredded material is put into the plastic bags that are included with the shredders. The purchase of an appropriate office shredder for the purpose of shredding confidential information is recommended. When a shredding bag is filled it must be placed in the appropriate venue for recycling.

6. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

7. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	CCTV Policy	Yogis Naicker

Document Shredding Policy

1. Overview

To define the policy related to the shredding of documents and related personal and confidential information. The scope of the Document Shredding Policy covers the whole of the business. This policy sets out how Block Secure (Pty) Ltd deals with paper documents that it is no longer required to store or is no longer allowed to store.

2. Policy

1. It is the responsibility of all employees and agents to:
    a. Ensure the security and confidentiality of personal information.
    b. Protect against anticipated threats to the security and/or integrity of such information.
    c. Guard against unauthorised access to or use of such records or information that could result in substantial harm or inconvenience to any data subject.
2. The reasons for shredding documents are:
    a. To ensure that personal information is safeguarded and not accessed by unauthorised individuals; and
    b. To encourage the efficient recycling of all printed materials.
3. If using off site shredding services, all shredding containers should be locked whilst awaiting emptying or collection. Documents to be shredded should be place in the appropriate container and should not be left to accumulate in offices. Only reputable shredding service providers shall be used.
4. For offices that shred their own documents, the shredded material is put into the plastic bags that are included with the shredders. The purchase of an appropriate office shredder for the purpose of shredding confidential information is recommended. When a shredding bag is filled it must be placed in the appropriate venue for recycling.

3. VII. Distribution

This policy is to be distributed to all Block Secure (Pty) Ltd staff and contractors using Block Secure (Pty) Ltd information resources.

4. Policy Version History

Version	Date	Description	Approved By
1.0	02/05/2024	Document Shredding Policy	Yogis Naicker