T: 082-005-8976 E: info@aubyte.co.za
W: www.aubyte.co.za
Cape Town, Western Cape
South Africa

Aubyte - Data Security and Privacy Policy

Effective Date: 25/06/2025

1. Purpose

This policy establishes the framework for protecting the confidentiality, integrity, and availability of all data handled by Aubyte. This includes our own corporate data, data belonging to our Managed Service Provider (MSP) partners, and, most critically, data belonging to our partners' end-clients. This policy is designed to ensure compliance with the Protection of Personal Information Act (POPIA) and other relevant regulations.

2. Scope

This policy applies to all Aubyte employees, contractors, and systems involved in the processing, storing, or transmitting of information.

3. Data Classification

- Level 3 (Confidential/Personal Information): Any data that can identify an individual (as defined by POPIA), client passwords, financial records, security configurations, and proprietary business information. This data requires the highest level of protection.
- Level 2 (Internal): Information for internal business use that does not contain personal information, such as project plans and internal communications.
- Level 1 (Public): Information already in the public domain.

4. Access Control

Access to data and systems will be granted based on the principle of "least privilege." Employees will only have access to the information and systems strictly necessary to perform their job duties for a specific task or project.

5. Data Handling and Protection

- All Confidential and Personal Information must be stored on Aubyte-approved, encrypted systems.
- Transmitting sensitive data over public networks must be done using encrypted protocols (e.g., VPN, SSL/TLS, SFTP).
- Storing client data on personal devices, unapproved cloud services (e.g., personal Google Drive), or removable media (like USB drives) is strictly prohibited without explicit, written management approval and appropriate security controls.
- Physical documents containing sensitive information must be secured when not in use and disposed of via approved shredding services.

6. Password Management
- All user accounts must be protected by strong, unique passwords.
- Passwords must not be shared, written down, or stored in plain text.
- Multi-Factor Authentication (MFA) must be enabled on all accounts and systems where available.

7. On-Site Security
- When working on-site, employees must lock their computer screens when leaving a device unattended.
- Employees must not leave any hardware, notes, or devices containing sensitive information in unsecured locations.

8. IT Asset Disposal (ITAD)
As a core service, our ITAD process must be impeccable.
- All storage media (HDDs, SSDs) from retired assets must be securely sanitized using methods that meet or exceed standards like NIST 800-88.
- Physical destruction will be used when data wiping is not possible or sufficient.
- Aubyte will provide a certificate of data destruction to the client upon completion.

9. Security Incident Response
Any suspected or confirmed data breach, security incident, or loss of a device must be reported immediately to Aubyte management. This allows us to take immediate action to mitigate harm and fulfill any legal notification requirements under POPIA.

10. Consequences of Violation
Failure to comply with this Data Security and Privacy Policy is a serious offense that may lead to disciplinary action, including immediate termination of employment and potential civil or criminal liability.

Acknowledgement:

Signature

25/06/2025

Date