Data Security – Leakage – Control - Policy

This Altitude Financial Solutions (Pty) Ltd policy sets out minimum security measures to prevent and detect violations from fines and lawsuits.

This document provides three data security policies that cover key areas of concern. They should not be considered an exhaustive list but rather each identify any additional areas that require policy in accordance with their users, data, regulatory environment, and other relevant factors.

1. Data security policy: Employee requirements

2. Data security policy: Data Leakage Prevention – Data in Motion

3. Data security policy: Workstation Full Disk Encryption

The purpose of this policy is to protect restricted, confidential, or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical. It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

1. Any employee, contractor or individual with access to systems or data needs to complete security awareness training and agree to uphold the acceptable use policy.
2. If you identify an unknown, un-escorted or otherwise unauthorized individual into the building you need to immediately notify building management and abide by control measures
3. Visitors to Altitude Financial Solutions must be always escorted by an authorized employee. If you are responsible for escorting visitors, you must restrict them to the appropriate areas.
4. You are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by Altitude Financial Solutions. For example, the use of external e-mail systems not hosted by Altitude Financial Solutions to distribute data is not allowed.
5. Please keep a clean desk. To maintain information security, you need to ensure that all printed documents in scope of data is not left unattended at your workstation.
6. You need to use a secure password on all systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
7. Terminated employees will be required to return all records, in any format, containing personal information. This requirement is part of your onboarding process and you have agreed and signed to accept this
8. You must immediately notify IT in the event that a device containing in scope data is lost (e.g. mobiles, laptops etc).
9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform IT or your direct line Manager so that they can take appropriate action.
10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from Management if you are unsure as to your responsibilities.
11. Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car.

12. Data that must be moved within is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). IT department will provide you with systems or devices that fit this purpose.
13. You must not use other mechanisms to handle in scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with IT or your direct line manager
14. Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from IT or your direct line Manager.

The IT team will conduct first level triage on events, identifying data that may be sensitive and situations where its transfer was authorized and there is a concern of inappropriate use. These events will be escalated to HR to be handled through the normal process and to protect the individual.

1. Where there is an active concern of data breach, the IT incident management process is to be used with specific notification provided to IT or HR.
2. Access to personal and confidential information will be restricted to Altitude Financial Solutions employees and approved third party storage providers only, to protect the privacy of clients.
3. High priority incidents discovered by IT should be immediately flagged with senior Management in the respective Business
4. Monthly reports showing % devices compliant with policy will be conducted
5. Workstation Full Disk Encryption is in place for all desktops and laptops
6. All machines report to the central management infrastructure to enable audit records to demonstrate compliance as required.
7. Where management is not possible and a standalone encryption is configured (only once approved by a risk assessment), the device user must provide a copy of the active encryption key to IT.
8. IT has the right to access any encrypted device for the purposes of investigation, maintenance or the absence of an employee with primary file system access to identify inappropriate access to systems or other malicious use. The help desk will be permitted to issue an out-of-band challenge/response to allow access to a system in the event of failure, lost credentials or other business blocking requirements. This challenge/response will be provided only in the event that the identity of the user can be established using challenge and response attributes documented in the password policy.
9. Regular security tests will be performed and documented identifying any areas of concern and remedial action that has been taken or is recommended.