ELANTAS

ELANTAS Beck India Ltd.

Information Security Policy V.7

Contents:

1.0 Overview

This security policy is a sub-set of the Altana Security Policy published on the Altana Intranet.

2.0 Aim

To define the information security guideline for ELANTAS Beck user's Data.

3.0 Data Privacy and User Authentication Policy

3.1 Data Privacy and Cyber Security

The objective of this policy is to uphold the confidentiality of and safeguard sensitive data and personal particulars pertaining to our workforce, contractors, suppliers, interns, collaborators, customers, and business associates (including vendors and distributors). Additionally, it aims to protect our IT assets against cyber risks and vulnerabilities. Within our context, sensitive data includes the following: Personal particulars, data/information relevant to business activities, communications exchanged between the company and its suppliers, vendors, and other business partners, data/information acquired through Non-Disclosure Agreements or confidentiality agreements, any data/information that holds confidentiality status as defined by applicable law, as well as any other data/information designated as confidential by the organization.

Responsibilities:

1. ALTANA Group has a Global Data Officer who interacts with the group entities for implementation of Data Privacy and Security.
2. Our employees, suppliers, contractors, other business partners, or anyone with data processing responsibility shall adhere to this policy and other legal data protection requirements as may be required from time to time.

Reporting: Stakeholders detecting or becoming aware of sensitive data breaches or their grievances, shall promptly notify Head IT & Infrastructure.

3.2 User Authentication Policy

- All users in a Local Area Network (LAN) shall be given permission for using Network resources using this Network Authentication Policy.
- Network Resources currently include Business Application Executables, email folders, shared folders on servers. These could be extended through notification from time to time.
- All users shall be assigned a distinct username along with a password without which access to network resources will not be available.
- The username shall follow the AC standard of E362 followed by first 3 characters of the last name followed by a serial number allotted by AC-IT.
- Users enter their user id and password for logging into the system from any desktop/ laptop resource.
- The password must adhere to following rules:

  Access to the ALTANA hardware and software and to the corporate network requires the entry of a personal login and password. Unless superseded by other (stricter) password requirements:

  1. The password must contain at least eight (8) characters, and must include figures and special characters in addition to letters.
  2. Common passwords such as names and birth dates, etc., that are easy to guess must not be used.
  3. Passwords must be changed at least every 180 days and previously used passwords should not be reused within 30 months.
- The password policy shall be enforced globally by Altana IT.

- To avoid dual forced authentication in a dual domain system the local domain can be accessed only by an equivalent username authenticated by the ACAG domain. The system uses a complicated algorithm to derive the password required by the local domain. Local domain authentication is enabled through separate passwords only for temporary staff and trainees, who do not have authentication on the ACAG domain.
- If a particular user account gets locked, or the password gets disabled, a request shall be made to IT department by logging a case in to service-now.
- A user required to change their initial password after their first logon.

4.0 New user creation and disablement of old user.

- The new user creation is done by HR Department in the software called Success factors. Once the HR department enters the new employee information in success factors. The user ID will be created with the automated process from success factors.
- For Employee, New username shall be allocated based on the request made by HR or the Admin Department in the prescribed format to the “service now” platform and approved by Head –IT.
- For External users, New username shall be allocated based on the request made by HR or the Admin Department, approved by the HOD in the prescribed format to the “service now platform” and approved by Head –IT.
- The IT Department will forward the service now request to group IT along with the necessary form for creating the new user in active directory.
- Upon receiving the intimation from the Service Desk, the IT team will administer the creation of user accounts, as required, in the local servers, and grant permissions to specified folders.

- The new username and initial password shall be communicated to the new user via telephone / mobile.
- The new user shall be requested to log on for the first time and change their initial password. The Network Administrator shall verbally confirm the completion of the process.
- When an employee leaves the organization, HR department will put the last date in success factors. The user ID for left employee will be disabled with the automated process from success factors.
- When an external user leaves the organization, HR/Admin must notify the IT department on such user's last working day. The IT department will then create a request to disable the user ID through the Altana Service Desk.
- For a temporary or external employee working with EBIL, IT Department will create a user id for a defined time period of maximum 6 months. After every six-month new request must be created for the extension of period by another six months or less. Corresponding department HOD needs to approve the extension request for user access. The process will involve using the service now requests.
- All share folder rights related to a user will be granted after submitting a new Service Now request with the approval from the folder's owner.

5.0 Hardware Use:

- Only hardware approved by ALTANA Group IT can be connected to the EBIL's internal network. Hardware belonging to external service providers must not be connected to the EBIL's Internal Network without approval from ALTANA Group IT.
- It is forbidden to connect and use private hardware (including private hardware components such as external hard disk drives, USB sticks, MP3 players, mobile telephones, etc.) on ALTANA hardware or the EBIL's Internal network.

- Non-ALTANA USB sticks such as those provided by a service provider may be connected to an ALTANA computer once the data contained on the stick is checked before use and found free of harmful software.
- EBIL IT has established a secure LAN connection using DHCP and VLAN to connect all hardware to Altana and the EBIL local network.
- Employees using ALTANA hardware must take reasonable steps to protect it against damage, loss, or theft.

6.0 Software Use:

- Only the software approved by ALTANA group IT should be used and installed on EBIL's local hardware.
- Software usage requires compliance with the software vendor's license conditions and intellectual property laws.
- All new installation of software will be conducted only by EBIL IT team only. Users are not allowed to install any software on their local hardware.

7.0 Internet & E-mail

- E-mail and Internet access provided by EBIL are strictly for official use only. These services may only be used for operational purposes unless exceptions are expressly granted in this policy.
- In all cases, including the case of permitted private use, all use of e-mail or Internet access that may compromise the interests of the ALTANA Group is strictly forbidden.
- Private commercial or other private business matters cannot be conducted using e-mail or Internet access.

- Private use of internet or data systems could be allowed with certain restrictions as may be imposed from time to time.
- The ALTANA Group reserves the right to limit the volume of data transmitted to and from the Internet and block access to specific websites or any other internet services.
- Internet access by users with administrator rights is prohibited.
- For security reasons, ALTANA hardware (e.g., PCs, laptops and servers) required to control production or logistics systems (SCADA systems, process control systems, etc.) will not be granted access to the Internet. ALTANA IT may grant exceptional authorization in justified situations where an exception is required for operational reasons.

8.0 Data Backup

- Data backup schedules and restoration audits will follow the EBIL Backup Policy, including storing backups in different fire zones.

9.0 Disposing of data media:

- Unused hardware and data media must be returned to EBIL IT for proper disposal. EBIL IT will ensure proper data destruction and deletion.

10.0 Guideline to users:

- All users shall maintain utmost secrecy of their passwords and must not share them with anyone for any reason whatsoever. Any such act of sharing passwords shall be a VIOLATION of this policy and shall attract disciplinary action.
- Users shall log into the system by entering their username and password. The entry of the password is invisible on the system. However, users must exercise reasonable care to enter the password in a secure manner, such that there is a minimal risk of any third party acquiring the password directly or indirectly. Example: enter the password in a single shot on the keyboard so that the sequence of keystrokes is not easily understood; avoid so far as possible, logging into the system when someone is observing your finger movements carefully etc.
- If a user doubts that the password being used by them is fully or partially known to someone else, it is advised to change the password immediately.
- Desktop systems should not be left unattended by a user after logging into the system. Users must log out /lock the machine for security, unless access to the desktop is physically secured in any other way, when not attended.
- Passwords can also be changed after periods of leave or out-of-office work if deemed necessary.

11.0 Periodic review by IT Personnel

Network administrators shall exercise special care in case of repetitive account lockouts. They shall periodically review password change logs and account locks and highlight repetitive cases to the Head IT for appropriate action.

User account reviews need to be conducted with the Head IT every six months.

12.0 Training and Awareness: IT security

There shall be training sessions on IT security and data privacy policy to cover topics on IT and cybersecurity with all users. These training sessions shall cover internal IT environment security needs along with data privacy rules and regulations, as well as security needs on IT in general, relevant to the needs of the organization. There shall be periodic communications to keep the awareness of IT security commensurate to the needs of the organization.

This Policy has been approved by the Board of Directors of ELANTAS Beck India Limited on 20th December, 2023 and is effective from this date.