salto

Onboarding Handbook

Revision History		
Date	**Author**	**Notes**
Mar 2021	Moran Carmel	Initial Version
Nov 2021	Gil Hoffer	Reviewed, amended and approved by Management
Jan 2022	Moran Carmel	Reviewed, amended and approved by Management

Table of Contents

Administrative

Responsibility

Supervision — Ensure compliance with the policy instructions

- CEO

Frequency

- This policy is reviewed on an annual basis.

Updates

- CEO

Addressees

- All Salto employees, Contractors and Consultants

In Effect

- This policy is valid from the day of publication.

Purpose

It is the responsibility of all Salto employees to protect sensitive data against loss or theft, as well as adhere to the company code of business conduct. Awareness, education and practice of the following guidelines can assist Salto to protect the company, its employees, customers, and contractors from damages related to the loss or misuse of sensitive information while keeping business integrity.

Password Policy Rules

Passwords are the gateway to Salto and its clients' most sensitive information. Therefore, passwords must be kept safe, and employees should use a password that is aligned with leading practices and hard to guess.

A strong password must:

- Be as long as possible (never shorter than 8 characters).
- Include mixed-case letters.
- Include digits and punctuation marks.
- Not be based on any personal information (e.g., employee name, date of birth, mobile number).
- Avoid using any dictionary word, in any language.
- Avoid using a sequence of numbers.
- Avoid using passwords that are used in third-party services (i.e., social networks).

In addition, employees must confirm they are aware that operations performed are logged and associated with the user who performed them.

Single Sign-On and MFA

Multi-Factor authentication (MFA) guarantees that the user attempting to log in has use of an associated mobile phone facilitating Salto to dramatically reduce the risk of credential theft. Employees must confirm they have activated the 2-step verification on all SaaS services (such as G-Suite, GitHub and AWS) and keep that feature activated until the account is closed.

Clear Desk

As sensitive data can also be distributed via hard copy or electronic means, employees must refrain from keeping unnecessary hard copies of Salto's intellectual property and customer data.

Email Security Rules

Beware of the following:

- Never open an attachment or click on any link in unexpected or suspicious emails.
- Never send any sensitive information via email, unless it is encrypted.
- Be suspicious of any email that requires executing unusual actions.
- Immediately report any unusual activity to your Manager or Salto's CEO.

Software Installation Rules

It is strictly forbidden to:

- Use pirated software
- Disable or tamper with any security measures deployed by Salto's IT

Appropriate Use of Computing Resources

Company employees are expected to use the Internet and any computer systems provided to them by the company responsibly and productively. All Internet data that is composed, stored, transmitted and/or received by Salto's computer systems is considered Salto's (or its respective clients') property and is thereby recognized as its official data. Therefore, the data is handled accordingly, subject to Salto's policies, contracts or disclosure to third parties for legal or other business reasons.

Make sure to:

- Encrypt your endpoint.
- Do NOT share confidential or proprietary company information on social media (e.g., OneDrive, Google Docs, pCloud etc.)

Incident Response - Employee Responsibility

Employees are responsible to report any irregular or suspicious activity in their accounts and working environments, such as:

- Unexplained account lockout
- Unusual last login time (in systems that provide this information)
- Signs of unknown activity (such as unknown files in their file areas or unexplained changes to desktop settings)
- Violation of information security procedures and instructions violations, either by the employee himself or by other employees
- Suspicion that information has been or might be damaged, disclosed, modified, or deleted
- Attempts (either failed or successful) to gain unauthorized access to the system or its data
- Unwanted disruption or denial of service
- Unauthorized use of the system for the processing or storage of data
- Customer reported suspicious activity or behavior
- Security alerts received from anti-virus software or phishing attempts

In case of a suspected incident, the CEO must be notified immediately.

Social Engineering Awareness

Social engineering is a form of fraud, aiming to manipulate people into performing actions or divulging confidential information. Social engineering can be presented in numerous forms, such as by phone, by email, social networks, chatting applications, or even in person, with the goal of obtaining confidential information or cause an employee to perform an action against the security policy of the company.

- Never provide any sensitive information, by phone, email or other means to anyone that contacts you from outside the company.
- Be suspicious of social engineering attempts.
- Immediately report any unusual activity (such as unaccompanied technicians) to your Manager or CEO.

Code of Business Conduct

A high level of credibility and integrity can only be maintained if every Salto employee is aware of their responsibility in compliance with Salto's Code of Business Conduct and Ethics. Therefore, all Company Personnel must conduct themselves accordingly and seek to avoid even the appearance of improper behavior. The purpose of the Code is to:

- Provide a general statement regarding the company's expectations of Company Personnel conduct, both legally and ethically.
- Promote honest and ethical conduct of all Company Personnel, including:
    - Ethical handling of conflicts of interest between personal and professional relationships.
    - Full, fair, accurate, timely and understandable disclosure in periodic reports required to be filed by the company.
    - Compliance with all applicable governmental rules and regulation.
    - Prompt internal reporting of Code violations.
    - Accountability for adherence to this Code.
    - NOT misrepresenting yourself or your company, or asking others to do so.
    - NOT making personal attacks or speaking negatively about Salto employees, interns, contractors, customers, suppliers, vendors, potential prospects, or competitors.

Employees shall promptly bring to Management's attention any information that they possess concerning:

- Significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting, which are likely to adversely affect the company's ability to record, process, summarize, and report financial information.
- Any fraud that involves Management or other company employees who play a significant role in maintaining the company's internal control over financial reporting.
- Any violation of this Code, including any actual or apparent conflicts of interest between personal and professional relationships, involving management or other employees who

play a significant role with respect to the Company's financial reporting or public disclosures, or in maintaining the company's internal controls.

Appendix A: Acknowledgment of Employee Handbook

Complete the following steps:

- Read the Employee Handbook.
- Sign and date the form, and hand it back to Human Resources.

By signing below, I agree that I have read and understood the “Onboarding Handbook” and agree to be bound by its terms.

Employee name: Michael Kirk DeBaets

Date: 27/ 03/ 2023

Signature: