1 Introduction

1.1 Policy Brief & Purpose

The purpose of this Cybersecurity policy is to describe our intent and stance towards information security, and we regard this necessary to ensure that due care is taken to avoid undue risk to Ac Goldman Solutions and Services Ltd (hereby Goldman Solutions or the "Company") its business partners and its stakeholders.

The Goldman Solutions Cybersecurity Policy outlines the guidelines and provisions for safeguarding the security of our data. As we increasingly rely on technology to collect, store, and manage information, we recognize the threats to security breaches. Human errors, cyber-attacks, and system malfunctions could cause significant financial damage and jeopardize our company's reputation.

To mitigate these risks, we have developed and established an Information Security Management System (ISMS) and implemented comprehensive security measures. We used existing and recognised Cybersecurity frameworks, i.e ISO 27001. This policy conforms with the National Cybersecurity Coordination Centre (NCC-CY) regarding the Cyberhygiene framework for SMEs in particular.

This policy encompasses provisions and additional commitments such as legal, regulatory, and contractual compliance. While we make every effort to protect from information risks, we believe that all Company's staff have a significant contribution when it comes to exercise the utmost vigilance for external threats hence, we continuously provide awareness training that makes sure our staff understand the mechanisms and build know-how to react in case of incidents

Before we decide on new systems, providers must among other things satisfy a set of security requirements.

Our processes are monitored at regular intervals making sure we comply with our ISMS requirements and other relevant (legal, regulatory) requirements relating to information security.

The Company's ISMS main objectives are described below:

- Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the Company using organisational, people, physical and technical controls.
- Provide value to the way we conduct business and support business objectives.
- Comply with all regulatory and legal requirements, including our stakeholders' expectations.
- Mature our security controls through embrace of Information Security best practices
- Contractual agreements that take into consideration the information risk exposure of the Company when certain processes are outsourced.

The objectives are supported by topic-specific policies, procedures guidelines, plans and other company mechanisms as described in this Policy.

The Information Security Management System is reviewed on annual basis or upon significant changes to the information security environment and it is audited so that areas of improvement are identified and implemented in a cycle of continuous improvement.

1.2 Scope

This policy applies to all Goldman Solutions employees, contractors, and anyone who has permanent or temporary access to our systems and hardware.

2 Security lMeasures - High Level

2.1 Confidential Data

Confidential data is secret and valuable. Examples include:

- Unpublished financial information
- Data of customers, partners, vendors
- Patents, formulas, or new technologies
- Customer lists (existing and prospective)

All employees, contractors, and anyone who has permanent or temporary access to our systems and hardware are obliged to protect this data. Specific instructions to avoid security breaches will be provided.

2.2 Protect Personal and Company Devices

When accessing company emails or accounts via personal or company-issued devices, employees introduce security risks. To mitigate these risks, employees should:

- Keep all devices password-protected.
- Use and regularly update comprehensive antivirus software.
- Avoid leaving devices exposed or unattended.
- Install security updates for browsers and systems monthly or as soon as they are available.
- Access company accounts and systems through secure and private networks only.
- Avoid using other people’s devices or lending their own devices to others.

Employees should follow these instructions and consult our Information Security Officer with any questions.

2.3 Keep Emails Safe

Emails often host scams and malicious software. To prevent virus infection or data theft, employees should:

- Avoid opening attachments or clicking on links without adequate explanation.

- Be wary of clickbait titles.
- Verify the legitimacy of email senders.
- Look for inconsistencies or suspicious indicators (e.g., grammar mistakes, excessive capitalization).

If unsure about an email's safety, employees should consult our IT Specialist.

2.4 Manage Passwords Properly

Password leaks are dangerous and can compromise our entire infrastructure. Employees should:

- Choose passwords with at least eight characters, including uppercase and lowercase letters, numbers, and symbols.
- Avoid using easily guessed information (e.g., birthdays).
- Remember passwords instead of writing them down. If written, passwords must be kept confidential and destroyed after use.
- Exchange credentials only when necessary, preferring phone communication with recognized individuals.
- Change passwords every two months.

To manage multiple passwords. Employees must create a secure password for this tool.

2.5 Transfer Data Securely

Data transfers introduce security risks. Employees must:

- Avoid transferring sensitive data unless necessary. For mass transfers, seek help from Security Specialists.
- Use the company network/system for sharing confidential data, avoiding public Wi-Fi.
- Ensure data recipients are authorized and have adequate security policies.

2.6 Report Scams, Privacy Breaches, and Hacking Attempts

Employees must report perceived attacks, suspicious emails, or phishing attempts immediately to our Chief Information Officer (CIO) and Information Security Officer. These specialists will investigate, resolve issues, and issue companywide alerts as necessary.

2.7 Additional Measures

To reduce security breach risks, employees should:

- Lock devices when leaving desks.
- Report stolen or damaged equipment promptly.
- Change all account passwords if a device is stolen.
- Report potential threats or security weaknesses.
- Avoid downloading unauthorized software.
- Refrain from accessing suspicious websites.
- Comply with our social media and internet usage policy.

3 Compliance with Digital Security Authority

Goldman Solutions is committed to complying with the criteria of the National Cybersecurity Coordination Centre (NCC-CY) regarding the Cyberhygiene framework for SMEs and the requirement of this policy and any future amendments and guidelines issued by the Digital Security Authority

4 Related Policies

Refer to the appropriate documents for detailed information on related policies:

- Privacy Policy
- Password Policy
- Back-Up Policy
- Network Security Policy

5 Senior Management Point of Contact

Management is responsible for establishing, communicating, and enforcing security policies and procedures. They must provide adequate resources and training to ensure the effective implementation of security controls.

The Information Security Officer is designated as the point of contact for cybersecurity issues, ensuring communication between stakeholders and the organization.

The Information Security Officer acts through the Information Security Officer.

6 Commitment to Timely Response and Corrective Actions

Goldman Solutions is committed to:

- Timely response to security incidents and relevant stakeholder notification.
- Implementing corrective or preventive actions as required by authorized parties (e.g., audit organizations).

7 Remote Employees

Remote employees must adhere to this policy, ensuring compliance with data encryption and protection standards. They are encouraged to seek advice from our Information Security Officer.

8 Disciplinary Action

Non-compliance with this policy may result in disciplinary action, ranging from verbal warnings and training for minor breaches to termination for severe or repeated breaches. Each incident will be examined on a case-by-case basis.

9 Improvement

Everyone at Goldman Solutions , from customers and partners to employees and contractors, must feel confident for the protection of their data.

By staying vigilant and prioritizing cybersecurity, we can maintain this trust and protect our systems and data infrastructure effectively. The Cybersecurity Policy is reviewed on annual basis or upon significant changes to the information security environment and it is audited so that areas of improvement are identified and implemented in a cycle of continuous improvement.