Information Security Policy

Policy Owner: Director, Cyber Security

Effective Date: July 31, 2023

Overview

This Information Security Policy is intended to protect Go1's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of Go1. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Go1 employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of Go1's information and assets. These rules are in place to protect customers, employees, and Go1. Inappropriate use exposes Go1 to risks including compromise of network systems and services, financial and reputational risk, and legal and compliance issues.

The Go1 "Information Security Policy" is comprised of this policy and all Go1 policies referenced and/or linked within this document.

Information Security Objectives

Information security objectives are set and monitored annually by Go1's ISMS Governance Council based upon a clear understanding of business requirements. The current information security objectives are as follows:

- Ensure the confidentiality, integrity and availability of Go1 customer, company and employee data
- Maintain an information security program that increases trust in Go1 as a secure SaaS provider
- Effectively manage third party supplier risk who process, store or transmit Go1 information Continually improve the security culture within Go1 to ensure staff are aware of the latest threats
- Achieve SOC 2 Type I & II certification Action plans to achieve these objectives are maintained and reviewed annually by the ISMS Governance Council.

Refer to 10 ISMS Information Security Objectives Plan for further details.

Leadership and Commitment

Go1 is dedicated to establishing, implementing, maintaining, and continually improving the ISMS. Leadership commitment is demonstrated by the ISMS Governance Council when carrying out their responsibilities as defined in the 03 ISMS Roles, Responsibilities, and Authorities document.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Go1 business or interact with internal networks and business systems, whether owned or leased by Go1, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Go1 and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Go1 policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultant and other workers at Go1, including all personnel affiliated with third parties. This policy applies to all Go1-controlled company and customer data as well as all equipment, systems, networks and software owned or leased by Go1.

Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents shall be reported immediately or as soon as possible by sending an email to security@go1.com.

In your email please describe the incident or observation along with any relevant details.

Whistleblower Policy

Go1 including its related companies (Company or Go1) is dedicated to the highest levels of ethics and integrity in the way we do business. Go1 encourages a culture of honest and ethical behaviour underpinned by the principles of good corporate governance. Go1 recognises the importance in identifying and reporting suspected unethical, illegal, or undesirable behaviour and encourages the disclosure of such information.

Go1 encourages a culture of honest and ethical behaviour underpinned by the principles of good corporate governance. Go1recognises the importance in identifying and reporting suspected unethical, illegal, or undesirable behaviour and encourages the disclosure of such information.

Anonymous reports may be submitted in line with the Whistleblower policy located here: https://go1.sharepoint.com/sites/Policies/SitePages/Whistle-blower-Policy-and-Process.aspx

Mobile Device Policy

Go1 employees may utilise personal (BYOD) mobile phones and/or tablets to access company systems or information. Go1 may prevent access to company systems or information from personal (BYOD) mobile phones and/or tablets as determined by the Information Security team, relevant system/information owner or executive management.

The following are recommended security controls that Go1 Information Security advises employees to implement when accessing Go1 systems or information on personal mobile phones and/or tablets:

- Ensure that devices are secured with a password/passcode or an equivalent control, such as biometrics (e.g., Apple FaceID)

- Always lock the devices when left unattended and set the screen to lock automatically after 5 minutes of inactivity
- Do not use jailbroken devices to access company systems or information, as Go1 may restrict access from such devices

When using personal (BYOD) mobile phones and/or tablets to access company systems or information, an employee must not download and/or store confidential information, including but not limited to customer data, on the devices or in personal cloud-based storage (e.g., iCloud). This guideline, however, does not apply to business contact information such as names, phone numbers, and email addresses.

Clear Screen Clear Desk Policy

Users shall not leave confidential materials unsecured on their desk or workspace, and will ensure that screens are locked when not in use.

Remote Access Policy

Laptops and other computer resources that are used to access Go1 systems or information must conform to the security requirements outlined in Go1's Information Security Policies and adhere to the following standards:

- Go1 owned laptops or desktops need to be registered with Go1 mobile device management (MDM) platform. This will ensure all applicable security controls are applied to the device
- Users are prohibited from changing or disabling any organisational security controls such as personal firewalls, antivirus software on systems used to access Go1 resources
- Unauthorised remote access technologies may not be used or installed on any Go1 system this includes personal VPNs
- Users should use mobile device tethering instead of connecting to public networks
- Access to any Go1 system or information is strictly prohibited from public computers

In the event a Go1 employee needs to use a personal laptop or desktop to access Go1 systems or information the following security requirements are required:

- Installed anti-virus/anti-malware software and an enabled firewall
- Latest operating system patches are installed
- All Go1 data is removed from the personal device when a Go1 owned device is received or at the end of employment

All exceptions to use personal laptops or desktops needs to be communicated to the Senior Manager, IT Operations and Director, Cyber Cyber Security.

Artificial Intelligence Technologies

The use of Artificial Intelligence (AI) technologies at work must align with Go1's ethical standards and business objectives. Employees are encouraged to leverage AI tools to enhance productivity, improve decision-making, and streamline workflows, provided that such use is transparent, fair, respects privacy and data security protocols, and the confidentiality of Go1's information. All AI-driven initiatives must be pre-approved by the relevant department leadership to ensure that such use complies with company policies and does not compromise proprietary information or operational integrity. Additionally, any use of AI must adhere to the Third Party Management Policy, ensuring that all third party AI services meet Go1's standards for security, compliance, and ethical considerations. You must not download AI applications on company devices, or share Go1 confidential information with any AI service without explicit company approval.

Acceptable Use Policy

Go1 proprietary and customer information stored on electronic and computing devices, whether owned or leased by Go1, the employee or a third party, remains the sole property of Go1 for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy. The use of Microsoft OneDrive (or similar technology provided by Go1) for business file storage is required for users of laptops or company issued devices.

You have a responsibility to promptly report the theft, loss, or unauthorised disclosure of Go1 proprietary information or equipment. You may access, use or share Go1 proprietary information only to the extent it is authorised and necessary to fulfil your role. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company-provided devices.

For security and network maintenance purposes, authorised individuals within Go1 may monitor equipment, systems and network traffic at any time.

Go1 reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities with properly documented Management approval. Under no circumstances is an employee of Go1 authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Go1 owned resources or while representing Go1 in any capacity. The list below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Go1
2. Unauthorized copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Go1 or the end user does not have an active license
3. Accessing data, a server, or an account for any purpose other than conducting Go1 business, even if you have authorised access, is prohibited
4. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, email bombs, etc.)
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home
6. Using a Go1 computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws
7. Making fraudulent offers of products, items, or services originating from any Go1 account
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section,

"disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes
9. Port scanning or security scanning is expressly prohibited unless prior notification to the Go1 Information Security team is made
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty
11. Circumventing user authentication or security of any host, network, or account
12. Introducing honeypots, honey nets, or similar technology on the Go1 network without the prior approval of the Go1 Information Security team.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means
15. Providing information about, or lists of: Go1 employees, contractors, partners, or customers to parties outside Go1 without authorisation

Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent the company and act accordingly.

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail", or other advertising material to individuals who did not specifically request such material (email spam)
2. Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages
3. Unauthorised use, or forging, of email header information
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies
5. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type
6. Use of unsolicited email originating from within Go1 networks or other service providers on behalf of, or to advertise, any service hosted by Go1 or connected via Go1's network

Additional Policies and Procedures Incorporated by Reference

Personnel are responsible for reading and complying with all policies relevant to their roles and responsibilities.

Role	Purpose
Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorised parties in accordance with business objectives.
Asset Management Policy	To identify organisational assets and define appropriate protection responsibilities.
Business Continuity & Disaster Recovery Plan	To prepare Go1 in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Data Management Policy	To ensure that information is classified and protected in accordance with its importance to the organisation.
Human Resources Policy	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.

Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Operations Security Policy	To ensure the correct and secure operation of information processing systems and facilities.
Physical Security Policy	To prevent unauthorised physical access or damage to the organisation's information and information processing facilities.
Risk Management Policy	To define the process for assessing and managing Go1's information security risks in order to achieve the company's business and information security objectives.
Secure Development Policy	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.
Third-Party Management Policy	To ensure protection of the organisation's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organisations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

Policy Compliance

Go1 will measure and verify compliance to this policy through various methods, including but not limited to ongoing monitoring, and both internal and external audits.

Exceptions

Requests for an exception to this policy must be submitted to the Information Security Manager for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Information Security Manager. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	April 11, 2022	Initial policy	Sara Spencer	John Lynch
2.0	August 23, 2022	Policy updates	Sara Spencer	John Lynch
3.0	August 23, 2022	Policy updates	Sara Spencer	John Lynch
4.0	March 10, 2023	Policy updates	John Lynch	John Lynch
5.0	March 10, 2023	Policy updates	John Lynch	John Lynch
6.0	March 28, 2023	Policy updates	John Lynch	John Lynch
7.0	March 30, 2023	Policy updates	John Lynch	Jon Ducrou
8.0	June 29, 2023	Policy updates	John Lynch	John Lynch
9.0	August 1, 2023	Moved from Drata and updated formatting and wording	Kyle Jackson	Jon Ducrou
9.1	August 23, 2024	Minor updates	Kristian Taylor	Gaurab Bhattacharjee

9.2	September 20, 2024	Minor updates	Kristian Taylor	Gaurab Bhattacharjee