Flo Software

Information Security Document

Data Security Policy

Version	Date	Description	Author
1.0	24th March 2023	Initial Distribution	Gary Marston

Introduction

This Data Security Policy is Flo Software's policy regarding the safeguarding and protection of sensitive personal information and confidential information as per cyber essentials standards.

Purpose

Flo Software is entrusted with the responsibility to provide services to clients who provide us with confidential information. Inherent in this responsibility is an obligation to provide strong protection against theft of data and all other forms of cyber threats.

The purpose of this policy is to establish standards for the base configuration, and acceptable use of equipment and any software running on it that is owned and/or operated by Flo Software or equipment that accesses Flo Software's internal systems.

Effective implementation of this policy will reduce the risk of unauthorized access to Flo Software proprietary information and technology and protect confidential client information.

Scope

This policy applies to equipment owned and/or operated by Flo Software, and to employees connecting to any Flo Software owned network domain or cloud applications that are used as part of projects or assignments managed by Flo Software.

Network/Server Security

Server Configuration Guidelines

- The most recent security patches must be installed on all systems as soon as it is feasible to do so, the only exception being when immediate application would interfere with business requirements.
- Servers should be physically located in an access-controlled environment or a cloud infrastructure environment with an IT infrastructure provider that has achieved and maintains a high level of compliance with IT standards such as ISO-27001.
- Servers are specifically prohibited from being operated from locations without appropriate physical access controls.
- All Client Instances are separate entities, lowering the risk of cross client data breaches.

Security-Related Events

Security-related events will be reported to the IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Evidence of port-scan or any other type of service scanning.
- Evidence of unauthorized access to privileged or non-privileged accounts.
- Service interruptions, error messages, or other anomalous occurrences such as that are not related to specific applications on the host.

Router Security

The following types of traffic should be disallowed using in the firewall configuration:

- IP directed broadcasts
- Incoming packets at the router sourced with invalid addresses such as RFC1918 address
- TCP small services
- UDP small services
- All source routing

Access rules are to be added only to meet the requirements of the network topography to sustain business operations. All changes made to the access rules of network devices must be documented in the location specified by IT management. The documentation must include the date and time that the changes were made and a detailed description of the process, including any shell commands executed to make the changes.

Password Security

Protective Measures

- Do not share Flo Software passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Flo Software information.
- Passwords should never be written down or stored anywhere online except in a password manager application that has been deemed acceptable by IT managers.
- Do not reveal a password in e-mail, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., “my family name”).
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the IT Department.
- Multi-factor authentication (MFA) MUST be enabled on all accounts that provide such a feature, and MFA codes MUST be stored in an MFA authenticator mobile application that has been deemed acceptable by IT managers. MFA backup codes should also be stored in a password manager to ensure their security, and if MFA backup codes are provided via a downloaded file, that file must be deleted, and purged from the trash-bin of the device.

Acceptable Use

General Use and Ownership

Any information deemed to be confidential or sensitive by Flo Software management, team leaders, or IT management should be encrypted as provided instructions from management.

For security and network maintenance purposes, authorized individuals within Flo Software may monitor equipment, systems and network traffic at any time.

Security and Proprietary Information

The information contained on Flo Software's systems should be classified as either confidential, sensitive, or public, as defined by corporate confidentiality guidelines. Employees should take all necessary steps to prevent unauthorized access to confidential and sensitive information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.

Unacceptable Use

The following activities are prohibited. The lists below are not exhaustive, but attempt to exemplify activities which fall into the category of unacceptable use.

- Under no circumstances is an employee of Flo Software authorized to engage in any illegal activity as defined under local, state, federal or international law while utilizing Flo Software owned resources.
- Violations of the rights of any person or corporation such as defamation, liable, trademark, copyright, patent or other intellectual property, trade secret, 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 Flo Software

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, ransomware, or other malware, etc.).
- 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.
- Activity that leads to 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 authorized to access.
- Port scanning or security scanning is expressly prohibited unless prior permission is granted by IT management.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is approved by the IT management and deemed part of the employee's normal job/duty.
- Circumventing or altering the normal user authentication process or security of any host, network or account.
- Interfering with or denying service to any user including the employee's own host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with any local network hosts or services or any external hosts or services via the Internet, whether or not they are owned and operated by Flo Software.
- Providing information about, or lists of, Flo Software data, internal hosts, or network configuration to parties outside Flo Software.
- Otherwise altering host or network configuration, or broadcasting any network communication data other than what is considered part of the employee's job/duty.

Encryption

Standards

- Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Encryption algorithms that are considered weak by IT security industry standards should not be used, and disabled in all applications.

- Key bit strength must be at least a minimum of 2048-bit keys for RSA public / private keypairs.
- Symmetric encryption for data-in-transit and data-at-rest must use AES 256-bit keys unless otherwise specified by IT management.
- Flo Software's allowed encryption algorithms and key length requirements will be reviewed annually and upgraded as technology allows.

Remote Access

Persons Affected

All Flo Software employees, consultants, vendors, contractors, and others who use mobile computing connecting to Flo Software's hosting network.

Requirements

- Secure remote access must be strictly controlled. Control will be enforced via one-time password or public/private keys and will always be supplemented when possible with multi-factor authentication (MFA) that supplies a one-time-password to an mobile MFA authenticator application that has been approved by the IT management. For information on creating a strong pass-phrase see the section IV Password Security policy.
- At no time should any Flo Software employee provide their login or e-mail password to anyone, inside or outside the organization. In the case that IT support needs to access an employee's account directly, the IT support shall change the user's password using admin privileges, and after finished, will provide the user with a temporary password, which will be required to be changed when the user accesses their account.
- All Windows desktop computers, laptops and workstations that are connected to Flo Software hosting network via remote access technologies must have approved and fully updated anti-virus software installed and configured to immediately scan all incoming files and configured to conduct a complete scan of all files on the device at least once per week.
- Individuals who wish to implement non-standard Remote Access solutions to the Flo Software production network must obtain prior approval from the IT department.

Data Retention

Reasons for Retention

Flo Software retains only that data that is necessary to effectively conduct its business operations and activities, and to remain compliant with applicable laws and regulations.

Reasons for data retention include:

- Providing ongoing services to registered users, customer, and clients
- Compliance with applicable laws and regulations associated with financial reporting by Flo Software to its funding agencies and other donors
- Compliance with applicable labour, tax and immigration laws
- Other regulatory requirements
- Compliance with industry standards certification
- Investigation of a security incident
- Restoration of data from a security incident
- Intellectual property preservation
- Defence against potential litigation

Data Retained

Flo Software has set the following specifications for types of data that shall be retained:

- Operational data related to project activities, project proposals, reporting and project management will be held for the period required by Flo Software.

- Client related data will be held in line with the Flo Software -> Client contract upon subscription to Flo services.
- See Flo Application – Data Backup Restore Security.docx for information detailing backup restore retention.