sawai Group IT Security Standard

1 Purpose and Scope

The purposes of this standard are to properly utilize and manage all digital information assets including IT systems in our business activities and assure security while complying with related internal policies and GxP regulations. All Sawai Group Holdings Co., Ltd. and its consolidated subsidiaries (hereinafter, “Sawai Group”) must comply with this standard. IT Departments in each region may prepare local policies and procedures in accordance with this standard to accommodate each region’s unique requirements. If an article/item in this standard is re-defined in local documents, it must be to make it stricter or more rigorous. The document structure diagram is shown at Appendix-1.

2 Roles and Responsibilities

- IT departments in Sawai Group companies is responsible for working collaboratively to establish management processes to manage and control all digital information assets and make efforts to improve its quality securing IT environment.
- It is the responsibility of all Sawai Group employees, contractors, guests, and other personnel granted access to Group issued computing devices or to IT Systems to become familiar with these standards and comply with the requirements set forth in this document.
- IT Management is responsible for the installation, configuration, and maintenance of systems, networks, devices, and other computing equipment and infrastructure including the oversight and direction of such activities. As part of these activities, IT department is responsible for appropriately securing these environments.
- IT Management is responsible for ensuring that all IT personnel granted access to computer rooms and equipment have appropriate education and experience to perform their job functions and are trained on this standard. Access is granted based on job description and is limited to only those with a defined business purpose.
- IT Management is responsible for regularly conducting IT security education and training so that all persons in Sawai Group companies can understand Group/local IT security policy, standards and related procedures.

3 Use of Digital Information Assets

All persons in Sawai Group companies shall utilize and manage digital information assets according to defined business purposes. All digital information assets shall be managed

according to the requirements and related regulations in each respective region.

All persons in Sawai Group companies are to be approved and authenticated to access digital information assets for business purposes only with appropriate credentials and authorization. A responsible person/department of digital information asset (hereinafter, “owner”) must set the minimum permission levels required for users and regularly monitor digital information access controls.

4 Use of Network and Communication Services

Sawai Group personnel access to internal and external network and communication services must be in accordance with defined rules and procedures. Access to digital information assets must be approved by the information owner or designee. Individual, unique user accounts must be assigned by authorized personnel. All Group issued computing devices shall use encrypted storage and have the capability to use encrypted transmission. All system access is protected via password or appropriate credentials.

In some cases it is permissible for an individual to use a non-Group issued device for business purposes and/or to access Company information. When a personal device is so used, the device is subject to local documents.

Sawai Group companies utilizing outside data center services including IT cloud model services must assure the confidentiality, integrity and availability of digital information assets stored there by appropriate means.

5 Data Protection

IT departments in Sawai Group companies shall implement appropriate measures to protect digital information asset confidentiality and mitigate leakage risk.

Data encryption is mandatory on Group issued devices and portable external storage devices (e.g. jump drives). Access to digital information assets from public places must use encrypted data transmission methods to prevent data leakage and unauthorized access.

Group devices are issued to a known user with a verifiable identity. Usage of IT devices and services are monitored for security purposes. It is expected that all systems and devices remain updated to the latest appropriate security patch levels, including anti-virus definitions to protect digital information assets. Computer screen idle time-out must not exceed 15 minutes.

Exceptions to the data protections stated in this document require approval by local IT Management.

6 Identity Controls

Domain user accounts are issued by the local IT department in line with defined

procedures. All users must be uniquely qualified and authenticated. Anonymous access to Sawai Group's digital information assets is not granted under any condition. Based on a security risk assessment, IT Management will determine if multi-factor authentication is required.

Domain Login Password Policy

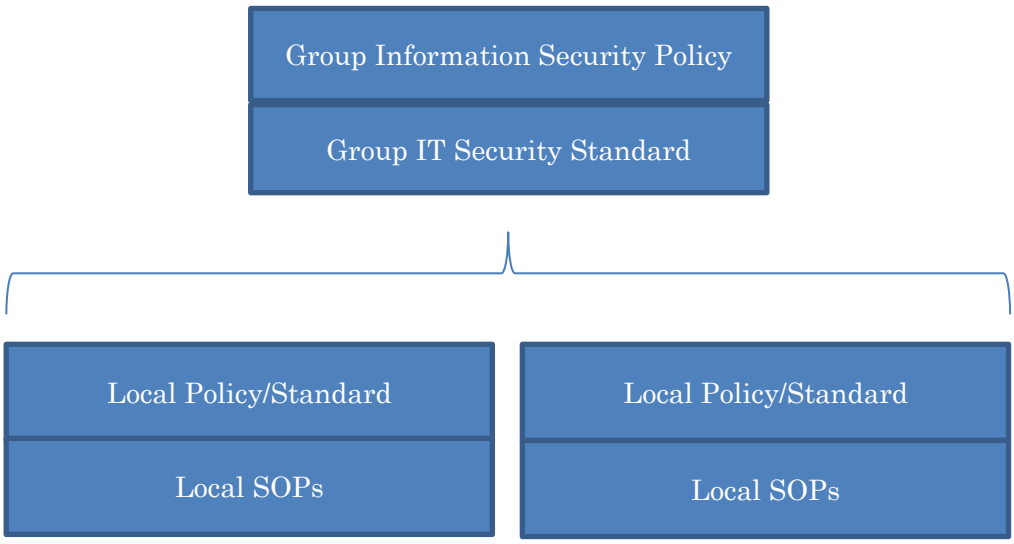
Length:	Minimum 8 characters
Complexity Rules:	Requires 3 of the following character types Capital Letter, Small Letter, Numeric, Non-Alphanumeric
Password Age	Maximum 90 days
Account Lock:	Maximum 10 failed login attempts cause account to lock within a defined time period

Default assigned passwords must be changed upon first user login. Passwords are not to be displayed on terminals, desks, or other openly accessible places. Account inventories are periodically reviewed to eliminate obsolete or stale items. Upon separation from the company, user accounts are immediately disabled.

7 Security Incident Management

Local IT departments shall establish its own IT security incident management and define procedures in local documents. As a global company, with inter-connected networks to encourage business collaboration and improve productivity, each IT department must make efforts to mitigate the potential to negatively impact other regions. In the event an incident impacts more than one region, each IT department shall perform a defined notification process, work together to solve, and report high severity level incidents to appropriate corporate information security officers in a timely manner. IT management shall conduct periodic reviews of actions taken to mitigate reoccurrences.

Appendix-1 Document Structure Diagram



Supplementary Provisions

This Policy shall be under the jurisdiction of the Group Chief Administrative Officer of Sawai Group Holdings.

The amendment and repeal of this Policy shall require the resolution of the Sawai Group Holdings Board of Directors.

Enacted and enforced on January 29, 2018

Revised and enforced on April 1, 2021

※Due to the transformation of Sawai Pharmaceutical into a holding company, the former Group policies of Sawai have been partially replaced and applied.