The Japanese version is the authoritative version, and this English translation is intended for reference purposes only. Should any discrepancies or doubts arise between the two versions, the Japanese version will prevail.

The Gakushuin School Corporation Information Security Policy

Effective as : 1st April 2017

I. Basic Information Security Policy

1. Principle and Purpose

In order for the Gakushuin School Corporation (hereinafter referred to as "Gakushuin") to promote educational and academic research and to carry out its social responsibilities, it is necessary to secure its information assets and enhance the information infrastructure.

Accordingly, the faculties, students, administrative personnel and other staff members of Gakushuin strive to improve the operational effectiveness of the Gakushuin information system. They are aware of the value its information assets and are committed to protecting and managing confidential information effectively and to preventing improper access or use of confidential information.

Gakushuin shall establish the "Gakushuin Information Security Policy" (hereinafter referred to as the "Policy") to fulfill the following objectives throughout Gakushuin. All users of information assets at Gakushuin (hereinafter referred to as the "Users") are to comply with the Policy, to prevent unauthorized access, alteration, destruction, reproduction, modification, and disclosure, whether intentionally or negligently, of both internal and external information assets of Gakushuin.

Gakushuin hereby declares to:

(1) protect the Gakushuin information system from unauthorized access.

(2) prevent any breach of internal and external information security.

(3) manage and maintain the operation of information assets.

(4) detect swiftly any breach in information security and take prompt corrective action.

2. Definition of terms

For the purposes of this policy, the following definitions shall apply:

(1) Information

Any documents, electronic documents and data in information systems which is created or collected by faculty members, office personnel and students for teaching, research, study and administrative activities, or any similar material.

(2) Information System

Any hardware, software, network, or recording equipment designed to process information, which is either owned or managed by Gakushuin, provided under contract by a third party, or connected to the Gakushuin network.

(3) Information Assets

Information and information management systems (data for information systems and systems development, operation, maintenance etc.).

(4) Information Security

Maintaining the confidentiality, the integrity, and the availability of information assets.

a. Confidentiality: All access to confidential information must be for authorized persons and for authorized purposes only.

b. Integrity: Information assets must not be destroyed, falsified or deleted.

c. Availability: Information must be accessible to authorized persons for authorized purposes when required.

3. Scope

(1) The Policy applies to the following:

a. Information assets owned or managed by Gakushuin.

b. Information assets managed by third parties under contractual or other arrangements with Gakushuin.

(2) The Policy applies to all users of information assets of Gakushuin (hereinafter referred to as "Users"). This includes executive officers, faculty members (including part-time lecturers), administrative office personnel (including ad hoc or part-time workers), joint researchers, students (including research students, credited auditors, scholarship students, and other special students,) and students, pupils, parents, guardians or guarantors, contractors and relevant external parties of Gakushuin educational system.

Ⅱ Information Security Programme Standards

1. Purpose

The programme standards outline the organisation structure, programme rules and standards necessary to fulfil the objectives of the Gakushuin information security policy.

2. Organisation and Structure

(1) Responsible Organisation and Administrators

To ensure information security, Gakushuin shall establish the following organisational structure (cf. Appendix - Organisation Chart):

a. Chief Information Security Officer

Gakushuin appoints the Executive Director of the General Affairs Division as the Chief Information Security Officer. The Chief Information Security Officer has executive (including internal and external) responsibility for information security policy.

b. Information Security Operational Manager

Gakushuin appoints as its Information Security Operational Managers the heads of the individual educational institutions as well as the Secretary General of the Administrative Section. Each Information Security Operational Manager is responsible for overseeing the information security of their division.

c. Departmental Information Security Manager

Gakushuin appoints the following bodies and individuals as its Departmental Information Managers, responsible for supervising information security arrangements (such as information devices, software and information) within their division, in order to ensure compliance with the Policy.

(a) University and Women's College

All Faculties who have authorized access to the information system through a client computer

(b) Boys' Senior High School, Boys' Junior High School, Girls' Senior High School, Girls' Junior High School, and Primary School.

Head of the Computer System

(c) Kindergarten

The Kindergarten Principal appoints the Information Manager

(d) Administrative Organisation

Director (the Deputy Director or Head will be appointed if the position of Director is vacant)

d. Network Administrator

Gakushuin appoints a Network Administrator to the Computer Centre and to the Computer Office of the General Affairs Division. The Network Administrators operate a core network system and major servers, and is responsible for the maintenance of the information security system.

e. Users are deemed responsible for the security of information assets owned and managed directly by them.

(2) Information Security Committee

Gakushuin appoints an Information Security Committee (hereinafter referred to as the "Committee") to promote information security programmes, and to manage the safe and effective operation of the information system.

The Committee will maintain and revise implementation regulations, monitor the protection of information assets, report any suspicion or claim of improper use of information assets, investigate security incidents and implement corrective measures.

The operations and procedures of the Committee will be stipulated by the Gakushuin Information Security Committee.

The General Affairs Section of the General Affairs Division will be responsible for the administrative work of the Committee.

3. Physical Security Controls

(1) Implementation of Information Systems

The Information Security Operational Managers shall supervise the implementation of important information systems such as servers and other devices and/or information assets in their respective divisions, and protect the systems from unauthorized access.

(2) Protecting information devices and recording media

The Information Security Operational Manager shall protect information devices and recording media from loss or theft.

(3) Off-Campus Use of Internal Information Devices and Recording Media

It is generally forbidden for Users to remove from Gakushuin any devices or recording media which contain personal information and sensitive data.

Should it become necessary to utilize information devices and/or recording media outside of Gakushuin, the Information Security Operational Manager must take security information measures so as to avoid any information exposure.

(4) On-Campus Use of External Information Devices and Recording Media

Users are required to take preventive information security measures, such as a virus check, if external information devices and recorded materials are used on campus.

(5) Information Backup

Users and Network Administrators periodically make backups of information data stored in servers and other devices.

(6) Disposal of Information Devices and Recording Media

When destroying or disposing of information devices and recording media, Users must ensure that the information is completely removed and cannot be retrieved by a third party.

4. Security Controls for Users

(1) Education and Training Seminar

The Chief Information Security Officer shall establish and maintain the Gakushuin information security management framework to ensure that all Users are trained in protecting confidential information.

(2) User Obligation

a. Users must acknowledge the importance of information security and adhere to the Policy and any other related rules and regulations in conducting their activities.

b. Users must not compromise Gakushuin information security either internally or externally.

c. Users must not access or use confidential Gakushuin information without authorization.

(3) Reporting Improper Use and Access

a. Users must report as soon as possible any breach or suspected breach of information security, or any security issues such as exposure, damage and alteration of Gakushuin confidential information to the Information Security Operational Manager, the Departmental Information Security Manager or to the Network Administrator.

b. The Network Administrator shall promptly investigate all reports or claims of a breach in information security regulations and/or unauthorized access to information.

c. The Network Administrator shall investigate the incident and take preventive measures such as disconnecting relevant communication devices, information systems and other actions, and report on the results of the investigation to the Information Security Operational Manager.

d. The Information Security Operational Manager shall report to the Chief Information Security Officer in the case of a serious information security incident.

e. The Chief Information Security Officer shall call a meeting of the Information Security Committee if a serious incident requires examination.

(4) Outsourcing Contract

When outsourcing work for developing and managing the information system, the Departmental Information Security Manager shall conclude an agreement of compliance with the third party, including subcontractors.

5. Technical Security Controls

Measures against unauthorized access

The Network Administrator shall provide access control functions in all information systems to protect against and to detect unauthorized access.

(1) Access Control

The Network Administrator shall designate users of information in accordance with its contents, and conduct effective access control to prevent unauthorized access.

(2) Saving Log Data

The Network Administrator shall determine the appropriate storage period and accordingly save the access log data of the system, operation log, etc.

(3) The Network Administrator shall be familiar with the information devices and software, and be committed to maintaining adequate security protection, such as anti-virus and security updates.

6. Responding to Incidents

Users who violate this Policy may be disciplined in accordance with relevant laws and regulations, with Gakushuin's employment policy, with Gakushuin's student and academic policies, etc.

7. Revision and Assessment of Information Securities Policies

Gakushuin shall periodically review the effectiveness of the Policy. Where necessary, the Policy shall be revised in accordance with the highest levels of information security and compliance.

Appendix: Organisation Chart