Swiss International Institute Lausanne

IT SECURITY POLICY

Swiss International Institute Lausanne - SIIL

Approved by:	Academic Council
Date of Approval:	01.10.2020
Date of Next Review:	01.09.2025
Owner:	IT Office
Contact:	p.tkachev@siil.ch

IT SECURITY POLICY

Swiss International Institute Lausanne - SIIL

Table of contents

I INTRODUCTION 4
II POLICY STATEMENT 4
III IT SECURITY GOVERNANCE 5
1. Governance outline 5
2. SIIL Data network 6
3. Autonomously Managed Networks 6
4. Authorised IT Support Area Representatives 6
5. Services to the SIIL Community 6
6. Communications 6

IV IT MANAGEMENT ROLES AND RESPONSIBILITIES 7
1. The SIIL Academic Council 7
2. Heads of Academic and Administrative Areas 7
3. The Information Security Officer 7
4. The Director of IT Services 7
5. Information Systems Users 7
6. Purchasing, Commissioning, Developing an Information System 8
7. Third Parties 8
8. Reporting of Security Incidents 8
9. Security Controls 8
10. Compliance with Legislation 8

V BREACHES OF SECURITY 9
1. Incident Reporting 9
2. Enforcement 9
3. Legal Implications 9
4. Disciplinary Procedures 9

VI POLICY AWARENESS AND DISTRIBUTION 9
1. New Staff and Students 9
2. Existing Staff 9
3. Logon Banner 10

4. Updates 10
5. Training 10
VII RISK ASSESSMENT AND COMPLIANCE 10
1. Risk Assessment 10
2. Heads of Academic and Administrative areas 10
3. Information Security Officer 10
4. Internal Audit 10
5. Third-Party Audit 10
VIII FURTHER INFORMATION 10

I INTRODUCTION

Information Security Policies are necessary to ensure that important teaching, research and administrative data, and other confidential information is protected from theft or unauthorised disclosure.

In addition to fulfilling legal obligations, complying with the policies will ensure that SIIL offers a professional and effective service.

All users of SIIL computing and networking facilities are expected to read and abide by the respective regulations.

II POLICY STATEMENT

Information is a critical asset of SIIL. Accurate, timely, relevant, and properly protected information is essential to the success of SIIL's academic and administrative activities. SIIL is committed to ensuring all accesses to, uses of, and processing of SIIL information is performed in a secure manner.

Technological Information Systems hereafter referred to as 'Information Systems' play a major role in supporting the day-to-day activities of SIIL. These Information Systems include but are not limited to all Infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store Information owned by SIIL.

The object of this Information Security Policy and its supporting technical requirements policy is to define the security controls necessary to safeguard SIIL Information Systems and ensure the security confidentiality and integrity of the information held therein.

The Policy provides a framework in which security threats to SIIL Information Systems can be identified and managed on a risk basis and establishes terms of reference, which are to ensure uniform implementation of Information security controls throughout SIIL.

SIIL recognises that failure to implement adequate Information security controls could potentially lead to

- Financial loss
- Irretrievable loss of Important SIIL Data
- Damage to the reputation of the SIIL
- Legal consequences

Therefore, measures must be in place, which will minimise the risk to SIIL from unauthorised modification, destruction or disclosure of data, whether accidental or deliberate. This can only be achieved if all staff and students observe the highest

standards of ethical, personal and professional conduct. Effective security is achieved by working with a proper discipline as well as in compliance with legislation and SIIL policies.

The Information Security Policy and supporting policies apply to all staff and students of SIIL and all other users authorised by SIIL.

The Information Security Policy and supporting policies do not form part of a formal contract of employment with the SIIL, but it is a condition of employment that employees will abide by the regulations and policies made by SIIL from time to time

The Information Systems Security Policy and supporting policies relate to the use of:

- All SIIL-owned/leased/rented and on-loan facilities.
- To all private systems, owned/leased/rented/on-loan, when connected to the SIIL network directly, or indirectly.
- To all SIIL-owned/licensed data/programs, on SIIL and on private systems.
- To all data/programmes provided to the SIIL by sponsors or external agencies.

The objectives of the Information Systems Security Policy and supporting policies are to:

- Ensure that information is created, used and maintained in a secure environment.
- Ensure that all of SIIL's computing facilities, programmes, data, network and equipment are adequately protected against loss, misuse or abuse.
- Ensure that all users are aware of and fully comply with the Policy Statement and the relevant supporting policies and procedures.
- Ensure that all users are aware of and fully comply with the relevant Swiss legislation.
- Create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure all SIIL-owned assets have an identified owner /administrator.

The SIIL Academic Council has approved the Information Security Policy and supporting technical policy. The Academic Council has delegated the implementation of the Information Security Policy, to the heads of academic and administrative areas.

III IT SECURITY GOVERNANCE

1. Governance outline

Security of SIIL's IT and data assets cannot be achieved without a coherent governance model that ensures that all IT systems in SIIL are operated in accordance with approved policy and best practice.

The SIIL Governance model seeks to clearly define who is authorised to operate key IT systems and services and how individuals and groups wishing to operate new systems or services are approved and subsequently governed.

2. SIIL Data network

This is the main SIIL network serving the entire staff and student population. This network is operated by IT Services and provides central services and support to all users.

The services of the main SIIL network are available to all users including users who are also members of other autonomously managed networks.

3. Autonomously Managed Networks

The autonomously managed networks (AMN's) are separate logical and physical networks created to address specific needs of a localised user population. They are operated under agreement with IT Services and managed by dedicated full time and suitably qualified staff. Each AMN appoints a named individual as the AMN manager. This person is responsible for authorising requests locally and liaising with IT Services.

4. Authorised IT Support Area Representatives

These individuals are employed by their academic or administrative area to spend a proportion of their time dealing with IT matters. These individuals may support specific applications and associated equipment.

5. Services to the SIIL Community

Only IT Services and the defined autonomous networks may operate central key central services including but not limited to Email, Internet Proxy, DNS, DHCP, Firewall, General Purpose Servers, Web Servers, Domain Services.

IT Support Representatives may operate specific applications and supporting servers which they should register with their AMN managers. End users or individuals - who are not employed by AMN's or as IT Support representatives - who wish to run complex IT systems such as servers should first seek approval from IT Services.

6. Communications

Good quality and frequent communications between all parties defined in this model are vital: Communications between Autonomous Networks and IT Support Representatives are facilitated by a mailing list and periodic meetings hosted by Information Systems Services.

IV IT MANAGEMENT ROLES AND RESPONSIBILITIES

1. The SIIL Academic Council

The SIIL Academic Council is responsible for approving the Information Security Policy, and for supporting the Director of IT Services in the enforcement of the policies where necessary.

2. Heads of Academic and Administrative Areas

Heads of academic and administrative areas are required to familiarise themselves with the policies. Where a policy breach is highlighted heads of academic and administrative areas must co-operate in ensuring that appropriate action is taken. Heads of academic and administrative areas are obliged to ensure that all IT systems under their remit are formally administered either by an administrator appointed by the head of an academic and administrative areas or centrally by IT Services. The duties of the administrator are set out in the associated supporting policy.

3. The Information Security Officer

The Information Security Officer is responsible for:

- Advising the Shareholders' Board, Academic Council, Management and other appropriate persons on compliance with this policy and its associated supporting policies and procedures.
- Reviewing and updating the Security policy and supporting policies and procedures.
- The promotion of the policy throughout SIIL.
- Periodical assessments of security controls as outlined in the Security Policy and supporting policies and procedures.
- Investigating Security Incidents as they arise.
- Maintaining Records of Security Incidents. These records will be encrypted and stored securely for six months after which time information pertaining to individuals will be removed. The records will then be held in this anonymous format for further two years for statistical purposes.
- Reporting to the Academic Council, Management and other appropriate persons on the status of security controls within the SIIL.

4. The Director of IT Services

The Director of IT Services or his/her deputy is responsible for the management of SIIL Network and for the provision of support and advice to all nominated individuals with responsibility for discharging these policies.

5. Information Systems Users

It is the responsibility of each individual Information Systems user to ensure his/her understanding of and compliance with this Policy.

All individuals are responsible for the security of SIIL Information Systems assigned to them. This includes but is not limited to infrastructure, networks, hardware and software. Users must ensure that any access to these assets, which they grant to others, is for SIIL use only, is not excessive and is maintained in an appropriate manner.

6. Purchasing, Commissioning, Developing an Information System

All individuals who purchase, commission or develop an Information System for SIIL are obliged to ensure that this system conforms to necessary security standards as defined in this Information Security Policy and supporting policies.

Individuals intending to collect, store or distribute data via an Information System must ensure that they conform to SIIL's defined policies and all relevant legislation.

7. Third Parties

Before any third-party users are permitted access to SIIL Information Systems, a written Third-party agreement is required. Prior to being allowed to work with SIIL Information systems, satisfactory references from reliable sources should be obtained and verified for all third parties which includes but is not limited to; administrative staff, software support companies, engineers, cleaners, contract and temporary appointments. Data processing, service and maintenance contracts should contain an indemnity clause that offers cover in case of fraud or damage. Independent third-party review of the adequacy of and compliance with information system controls must be periodically obtained.

8. Reporting of Security Incidents

All suspected information security incidents must be reported as quickly as possible through the appropriate channels. All SIIL staff and students have a duty to report information security violations and problems to the Information Security Officer on a timely basis so that prompt remedial action may be taken. The Information Security Officer will be responsible for setting up an Incident Management Team to deal with all incidents. Records describing all reported information security problems and violations will be created. These records will be encrypted and stored securely for six months after which time all information pertaining to individuals will be removed. The records will be held in this anonymous format for further two years for statistical purposes.

9. Security Controls

All SIIL Information Systems are subject to the information security standards as outlined in this and related policy documents. No exceptions are permitted unless it can be demonstrated that the costs of using a standard exceed the benefits, or that the use of a standard will clearly impede SIIL activities.

10. Compliance with Legislation

SIIL has an obligation to abide by all Swiss legislation and relevant legislation of the European Community if applicable. The relevant acts, which apply in Swiss law to Information Systems Security, include also The General Data Protection Regulation (GDPR).

V BREACHES OF SECURITY

1. Incident Reporting

Any individual suspecting that there has been, or is likely to be, a breach of information systems security should inform the Information Security Officer or the Director of IT Services immediately who will advise SIIL on what action should be taken.

2. Enforcement

The Director of IT Services or his/her delegated agent has the authority to invoke the appropriate disciplinary procedures to protect SIIL against breaches of security. In the event of a suspected or actual breach of security, the Director of IT Services, his/her delegated agent or the Information Security Officer may, after consultation with the relevant Administrator make inaccessible/remove any unsafe user accounts, data and/or programs on the system from the network.

3. Legal Implications

Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of Swiss legislation or the General Data Protection Regulation (GDPR) (if applicable) and could lead to civil or criminal proceedings and/or regulator fines. All staff and students are advised to familiarise themselves with and comply with this policy and with the SIIL Data Protection Policy.

4. Disciplinary Procedures

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken.
Failure of a contractor to comply could lead to the cancellation of a contract.

VI POLICY AWARENESS AND DISTRIBUTION

1. New Staff and Students

This Policy Statement will be available from IT Services on request. It will also be published on the IT page of SIIL website. New staff and students will be notified of the relevant policy documents on commencement of employment or student registration.

2. Existing Staff

Existing staff and students of SIIL, authorised third parties and contractors given access to the SIIL network will be advised of the existence of this policy statement.

They will also be advised of the availability of the associated policies and procedures which are published on the IT Services website.

3. Logon Banner

Users logging onto the SIIL network will be reminded of their obligations regarding compliance with the Information Security Policy via a Logon banner.

4. Updates

Updates to Policies and procedures will be made periodically and will be posted to the IT Services web site.

5. Training

Training will be available from IT Services. Further information can be accessed on the IT Services website.

VII RISK ASSESSMENT AND COMPLIANCE

1. Risk Assessment

Risk assessments must be carried out periodically on the business value of the information users are handling and the information systems security controls currently in place. This is to take into account changes to operating systems, business requirements, and SIIL priorities, as well as relevant legislation and to revise their security arrangements accordingly.

2. Heads of Academic and Administrative areas

Heads of academic and administrative areas must establish effective contingency plans appropriate to the outcome of any risk assessment.

3. Information Security Officer

The Information Security Officer will carry out risk assessments, review all risk assessments completed by other parties and highlight any measures needed to reduce risk in Information Security areas.

4. Internal Audit

The SIIL Internal Auditor will facilitate the assessment of risk management and compliance with the Information Security Policy periodically.

5. Third-Party Audit

Third-Party Audits will be carried out at intervals, as deemed necessary by the Internal Auditor an/or the Director of IT Services

VIII FURTHER INFORMATION

Specific queries on this policy or requests should be directed to the IT Services department (email: p.tkachev@siil.ch), who will progress as appropriate.

Approved by:	Academic Council
Date of Approval:	01.09.2020
Date of Next Review:	01.09.2025
Owner:	IT Office
Contact:	p.tkachev@siil.ch