Swiss International
Institute Lausanne

ПОЛИТИКА ПО БЕЗОПАСНОСТИ ИТ

Швейцарский международный институт Лозанны – SIIL

Утверждено:	Академический Совет
Дата утверждения:	01.10.2020
Дата пересмотра:	01.09.2025
Ответственный:	Отдел ИТ
Контактное лицо:	p.tkachev@siil.ch

Grand'Rue 92, 1820 Montreux, Switzerland
+41 31 520-70-82 • info@siil.ch • https://siil.ch

ПОЛИТИКА ПО БЕЗОПАСНОСТИ ИТ

Швейцарский международный институт Лозанны – SIIL

Содержание

I ВВЕДЕНИЕ

Политики по информационной безопасности необходимы, чтобы обеспечить защиту важных данных о преподавании, научных исследованиях и административных процессах, а также другой конфиденциальной информации от кражи или несанкционированного разглашения.

Помимо выполнения юридических обязательств, соблюдение настоящей Политики обеспечит профессиональное и действенное оказание услуг в SIIL.

Все пользователи вычислительных средств и сетевых объектов SIIL обязаны ознакомиться с соответствующими нормами и выполнять их.

II ДЕКЛАРАЦИЯ ПРИНЦИПОВ

Информация – важнейший актив SIIL. Достоверная, актуальная, релевантная и должным образом защищенная информация необходима для успешной академической и административной деятельности SIIL. Институт обязуется обеспечить доступ к информации SIIL, ее использование и обработку исключительно безопасным образом.

Технологические информационные системы, здесь и далее именуемые «информационные системы», играют большую роль в обеспечении повседневной деятельности SIIL. Эти информационные системы включают, без ограничения, всю инфраструктуру, сети, аппаратное и программное обеспечение, используемое для обращения с информацией, которой владеет SIIL, ее обработки, передачи или хранения.

Целью настоящей Политики по информационной безопасности и вспомогательной политики по техническим требованиям является определение мер контроля безопасности, необходимых для защиты информационных систем SIIL, и обеспечение безопасности, конфиденциальности и целостности хранящейся в них информации.

В настоящей Политике представлена структура, позволяющая идентифицировать угрозы безопасности информационных систем SIIL и управлять ими исходя из рисков; здесь также составлено техническое задание, обеспечивающее единообразное применение мер контроля безопасности информации во всех подразделениях SIIL.

SIIL осознает, что отсутствие надлежащих средств контроля безопасности информации может потенциально вызвать:

- Финансовый ущерб;
- Невосполнимую потерю важных данных SIIL;

- Ущерб для репутации SIIL;
- Правовые последствия.

В связи с этим необходимо принять меры, минимизирующие риск для SIIL в случае несанкционированной модификации, уничтожения или разглашения данных, будь то случайного или намеренного. Достичь этой цели можно только при условии, что все сотрудники и студенты будут придерживаться высочайших этических стандартов поведения в личной и профессиональной жизни. Для действенной защиты необходима надлежащая дисциплина в работе, соблюдение законов и выполнение политик SIIL.

Политику по информационной безопасности и вспомогательные политики обязаны выполнять все сотрудники и студенты SIIL, а также все прочие пользователи, уполномоченные SIIL.

Политика по информационной безопасности и вспомогательные политики не являются частью официального трудового договора с SIIL, однако являются условием трудоустройства, согласно которому сотрудники должны следовать регламентам и политикам, составляемым SIIL.

Политика по безопасности информационных систем и вспомогательные политики касаются использования:

- Всех объектов, находящихся в собственности SIIL, арендованных, сданных в аренду или предоставленных на время;
- Всех частных систем, находящихся в собственности, арендованных, сданных в аренду или предоставленных на время, при подключении к сети SIIL напрямую или опосредованно;
- Всех данных/программ, находящихся в собственности SIIL, на системах SIIL и частных системах;
- Всех данных/программ, предоставленных SIIL спонсорами или внешними сторонами.

Задачи Политики по безопасности информационных систем и вспомогательных политик:

- Обеспечить создание, использование и сохранение всей информации в безопасных условиях;
- Обеспечить надлежащую защиту всех вычислительных мощностей, программ, данных, сетей и оборудования SIIL от потери, неправомерного использования или злоупотребления;
- Обеспечить знакомство всех пользователей с декларацией принципов и соответствующими вспомогательными политиками и процедурами и полное выполнение этих норм;
- Обеспечить знакомство всех пользователей с соответствующим законодательством Швейцарии и полное его соблюдение;

- Донести информацию о необходимости использования надлежащих мер безопасности как элемента обеспечения и поддержки информационной безопасности;
- Обеспечить понимание всеми пользователями своих обязанностей по защите конфиденциальности и целостности данных, с которыми они работают;
- Обеспечить наличие установленного владельца/администратора всех активов, находящихся в собственности SIIL.

Академический совет SIIL утвердил Политику по информационной безопасности и вспомогательную техническую политику. Академический совет поручил реализацию Политики по информационной безопасности руководителям академических и административных подразделений.

III ОБЩЕЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ИТ

1. Описание управления

Безопасность ИТ и массивов данных SIIL была бы невозможна без гармоничной модели управления, обеспечивающей эксплуатацию всех ИТ-систем SIIL в соответствии с утвержденной политикой и лучшей практикой.

Модель управления SIIL создана с целью четкого определения лиц, уполномоченных эксплуатировать основные ИТ-системы и сервисы, и способов утверждения физических лиц и групп, желающих эксплуатировать новые системы и услуги, а также последующего управления такими лицами и группами.

2. Сеть данных SIIL

Это главная сеть SIIL, предоставляющая услуги всем сотрудникам и студентам. Ее эксплуатацией занимается Отдел ИТ-услуг и поддержки, который обеспечивает централизованное оказание услуг и предоставляет поддержку всем пользователям.

Сервисы главной сети SIIL доступны всем пользователям, в том числе тем, которые также используют автономно управляемые сети.

3. Автономно управляемые сети

Автономно управляемые сети (АУС) – это отдельные логические и физические сети, созданные для удовлетворения конкретных потребностей отдельных категорий пользователей. Эксплуатация таких сетей осуществляется на основании соглашения между Отдел ИТ-услуг и поддержки; управлением сетями занимаются выделенные сотрудники, занятые на полный рабочий день и обладающие необходимыми компетенциями. Для каждой АУС назначается

конкретное лицо, которое в качестве руководителя АУС отвечает за локальную выдачу разрешений на запросы и взаимодействие с Отдел ИТ-услуг и поддержки.

4. Уполномоченные представители, оказывающие ИТ-поддержку по направлениям

Лица, которые посвящают часть своего рабочего времени решению вопросов, связанных с ИТ, привлекают соответствующие академические или административные подразделения. Они могут оказывать поддержку по конкретным приложениям и сопутствующему оборудованию.

5. Услуги для сообщества SIIL

С централизованными ключевыми сервисами, к которым относятся, без ограничения, электронная почта, прокси-серверы, сервер доменных имен (DNS), протокол динамической настройки узла (DHCP), файрвол, серверы общего назначения, веб-серверы и доменные службы, имеет право работать только Отдел ИТ-услуг и поддержки и установленные автономные сети.

Представители, оказывающие ИТ-поддержку, могут работать с конкретными приложениями и вспомогательными серверами, зарегистрировав их с участием руководителей своих АУС. Конечные пользователи или физические лица (не являющиеся сотрудниками, обслуживающими АУС, или представителями, оказывающими ИТ-поддержку), которые желают управлять сложными ИТ-системами, такими как сервера, должны предварительно согласовать это с Отделом ИТ-услуг и поддержки.

6. Коммуникации

Качественные и частые коммуникации между всеми сторонами, включенными в эту модель, жизненно необходимы. Обмен информацией между автономными сетями и представителями, оказывающими ИТ-поддержку, осуществляется в рассылке по электронной почте и на совещаниях, периодически организуемых Отделом ИТ-услуг и поддержки.

IV РОЛИ И ОБЯЗАННОСТИ ПО УПРАВЛЕНИЮ ИТ

1. Академический совет SIIL

Академический совет SIIL отвечает за утверждение Политики по информационной безопасности и по мере необходимости содействует Директору Отдела ИТ-услуг и поддержки в обеспечении соблюдения политик.

2. Руководители академических и административных подразделений

Руководители академических и административных подразделений обязаны ознакомиться с настоящими политиками. При обнаружении нарушения политики руководители академических и административных подразделений должны содействовать принятию надлежащих мер. Руководители академических и административных подразделений обязаны обеспечить формальное администрирование всех ИТ-систем, находящихся в их ведении, либо администратором, назначенным руководителем академического или административного подразделения, либо централизованно Отделом ИТ-услуг и поддержки. Обязанности администратора установлены в соответствующей вспомогательной политике.

3. Менеджер по информационной безопасности

Медежер по информационной безопасности отвечает за:

- Консультирование Совета акционеров, Академического совета, руководителей и других соответствующих лиц относительно выполнения настоящей политики и сопутствующих вспомогательных политик и процедур;
- Пересмотр и актуализацию Политики по безопасности и вспомогательных политик и процедур;
- Донесение этой Политике до всех подразделений SIIL;
- Периодическую оценку средств контроля безопасности, перечисленных в Политике по безопасности и вспомогательных политиках и процедурах;
- Расследование происшествий в сфере безопасности в случае их появления;
- Ведение учетных данных по происшествиям в сфере безопасности. Эти данные хранятся в безопасном месте в зашифрованном виде в течение шести месяцев, после чего информация, касающаяся физических лиц, удаляется. Далее записи хранятся в анонимизированном виде в течение еще двух лет в статистических целях.
- Отчетность перед Академическим советом, руководителями и другими соответствующими лицами относительно состояния средств контроля безопасности в SIIL.

4. Начальник Отдела ИТ-услуг

Начальник Отдела ИТ-услуг и поддержки и его/ее заместитель отвечает за управление сетью SIIL и предоставление поддержки и консультаций всем назначенным сотрудникам, в обязанности которых входит реализация этих политик.

5. Пользователи информационных систем

Каждый пользователь информационных систем отвечает за свое понимание и соблюдение настоящей Политики.

Все физические лица отвечают за безопасность порученных им информационных систем SIIL, к которым относятся, без ограничения, инфраструктура, сети, аппаратное и программное обеспечение. Пользователи должны убедиться, что предоставляемый ими другим лицам доступ к этим объектам предназначен только для использования в интересах SIIL, не является избыточным и надлежащим образом поддерживается.

6. Закупка, ввод в эксплуатацию и развитие информационной системы

Все физические лица, закупающие, вводящие в эксплуатацию или развивающие какую-либо информационную систему для SIIL, должны убедиться, что эта система соответствует необходимым стандартам безопасности, установленным в настоящей Политике информационной безопасности и вспомогательных политиках.

Физические лица, намеревающиеся собирать, хранить или распространять данные через информационную систему, должны убедиться в соблюдении установленных политик SIIL и всех применимых законов.

7. Третьи стороны

До предоставления доступа к информационным системам SIIL каким-либо третьим сторонам необходимо заключить с этой третьей стороной соглашение в письменной форме. Прежде чем предоставить разрешение на работу с информационными системами SIIL, необходимо получить из надежных источников удовлетворительные и подтвержденные отзывы обо всех третьих сторонах, к которым относятся, без ограничения, административный персонал, компании – разработчики программного обеспечения, инженеры, уборщики, временные работники и подрядчики. Договоры на обработку данных, оказание услуг и обслуживание должны включать положение об освобождении об ответственности, согласно которому SIIL будет огражден от исков о мошенничестве или ущербе. Периодически необходимо привлекать независимую третью сторону для анализа пригодности средств контроля информационных систем и выполнения правил их применения.

8. Отчетность о происшествиях в области безопасности

Обо всех предполагаемых происшествиях в области информационной безопасности необходимо как можно скорее сообщать через соответствующие каналы. Все сотрудники и студенты SIIL обязаны своевременно информировать Менеджера по информационной безопасности о нарушениях информационной безопасности и проблемах в этой области, чтобы можно было оперативно принять корректирующие меры. Менеджер по информационной безопасности отвечает за формирование группы реагирования на происшествия для работы по каждому происшествию. По всем сообщениям о проблемах и нарушениях в сфере информационной безопасности создаются записи с их описанием. Эти записи хранятся в зашифрованном и защищенном виде в течение шести месяцев, после чего все сведения, относящиеся к физическим лицам, удаляются. Затем записи хранятся в анонимизированной форме в течение еще двух лет в статистических целях.

9. Средства контроля безопасности

Стандарты информационной безопасности, изложенные в настоящей Политике и сопутствующих документах, касаются всех информационных систем SIIL. Исключения допускаются только при возможности доказать, что расходы на применение стандарта превышают выгоды от него или что применение какого-либо стандарта очевидным образом мешает деятельности SIIL.

10. Соблюдение законодательства

SIIL обязан соблюдать все законы Швейцарии и применимые законы Европейского сообщества в этой сфере. К нормативно-правовым актам в сфере безопасности информационных систем, действующим в законодательной системе Швейцарии, относится также Законе о защите данных (GDPR).

V НАРУШЕНИЕ БЕЗОПАСНОСТИ

1. Отчетность о происшествиях

Физическое лицо, подозревающее о произошедшем или вероятном нарушении безопасности информационных систем, обязано немедленно проинформировать Менеджера по информационной безопасности или Начальника Отдела ИТ-услуг и поддержки, который порекомендует SIIL, какие действия необходимо предпринять.

2. Взыскания

Начальник Отдела ИТ-услуг и поддержки или его/его уполномоченный имеет право налагать соответствующие дисциплинарные взыскания для защиты SIIL от нарушения безопасности. В случае подозреваемого или реального нарушения безопасности Начальник Отдела ИТ-услуг и поддержки, его уполномоченный или Менеджер по информационной безопасности может, проконсультировавшись с соответствующим администратором, сделать недоступными / удалить из сети все небезопасные аккаунты пользователей, данные и/или программы системы.

3. Правовые последствия

Любое нарушение безопасности какой-либо информационной системы может привести к утрате безопасности персональной информации. Это нарушает законодательство Швейцарии и/или Закон о защите данных (GDPR), если он применим, что может стать поводом для возбуждения гражданских или уголовных дел и/или штрафам со стороны регулирующих органов. Всем сотрудникам и студентам рекомендуется ознакомиться с настоящей Политикой и Политикой по защите данных SIIL и соблюдать их.

4. Дисциплинарные меры

Несоблюдение настоящей Политики отдельным студентом или сотрудником может привести к наложению соответствующих дисциплинарных взысканий, а в некоторых случаях – к обращению в суд.
Несоблюдение подрядчиком этих требований может стать причиной расторжения договора.

VI ЗНАКОМСТВО С ПОЛИТИКОЙ И ЕЕ РАСПРОСТРАНЕНИЕ

1. Новые сотрудники и студенты

Настоящую декларацию принципов можно получить по запросу в Отделе ИТ-услуг и поддержки. Она также будет выложена на посвященной ИТ странице на веб-сайте SIIL. Новые сотрудники и студенты уведомляются о соответствующих регулирующих документах в момент начала работы или зачисления.

2. Нынешние сотрудники

Нынешние сотрудники и студенты SIIL, уполномоченные третьи стороны и подрядчики, которым предоставлен доступ к сети SIIL, уведомляются о существовании настоящей декларации принципов. Они также уведомляются о наличии сопутствующих политик и процедур, публикуемых на веб-странице Отдела ИТ-услуг и поддержки.

3. Графическая заставка при входе в сеть

Пользователи, выполняющие вход в сеть SIIL, будут видеть напоминание о своих обязанностях по соблюдению настоящей Политики по информационной безопасности в графической заставке при входе в сеть.

4. Обновления

Политики и процедуры будут периодически обновляться; новые версии будут выкладываться на веб-странице Отдела ИТ-услуг и поддержки.

5. Обучение

Отдел ИТ-услуг и поддержки проводит обучение. С дополнительной информацией можно ознакомиться на веб-странице Отдела ИТ-услуг и поддержки.

VII ОЦЕНКА РИСКОВ И СОБЛЮДЕНИЕ НОРМ

1. Оценка рисков

Необходимо периодически проводить оценку рисков для сопоставления ценности для бизнеса информации, которой оперируют пользователи, и ныне существующих средств контроля безопасности информационных систем. При такой оценке учитываются изменения в операционных системах, требованиях бизнеса и приоритетах SIIL, а также в применимом законодательстве, а меры безопасности пересматриваются в соответствии с ними.

2. Руководители академических и административных подразделений

По итогам оценки рисков руководители академических и административных подразделений должны разработать эффективные планы действий в случае чрезвычайной ситуации.

3. Менеджер по информационной безопасности

Менеджер по информационной безопасности проводит оценку рисков, анализирует оценку рисков, выполненную другими сторонами, и указывает меры, которые необходимо принять для снижения рисков в сферах информационной безопасности.

4. Внутренний аудит

Внутренний аудитор SIIL периодически организует оценку управления рисками и соблюдения Политики по информационной безопасности.

5. Внешний аудит

Внешние аудиты проводятся с определенной периодичностью, которую устанавливает внутренний аудитор и/или Начальник Отдела ИТ-услуг и поддержки.

VIII ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Вопросы относительно данной политики и запросы следует направлять в Отдел ИТ-услуг и поддержки (email: p.tkachev@siil.ch), который обрабатывает их в зависимости от ситуации.

Утверждено:	Академический Совет
Дата утверждения:	01.10.2020
Дата пересмотра:	01.09.2025
Ответственный:	Отдел ИТ
Контактное лицо:	p.tkachev@siil.ch