Logging, Analysis and Monitoring of Log-Data at ETH Zurich

of 01 January 2025

1. Section: General provisions 2
Article 1 Subject matter 2
Article 2 Applicability 2
Article 3 Goal and purpose 3

2. Section: Logging 3
Article 4 Proper logging 3
Article 5 Contents to be logged 3

3. Section: Analysis 4
Article 6 Proper analysis 4
Article 7 Non-personalised analysis 4
Article 8 Non-nominal personalised analysis 5
Article 9 Nominal personalised analysis (by name) 5

4. Section: Technical monitoring 6
Article 10 Monitoring and scanning of vulnerabilities 6

5. Section: Storage and deletion 6
Article 11 Deletion periods 6
Article 12 Analyses 7

6. Section: Centralised storage in the CISEC log container 7
Article 13 Forwarding of log data 7

7. Section: Security requirements 8
Article 14 Confidentiality 8
Article 15 Integrity 8
Article 16 Availability 8

8. Section: Duties 9
Article 17 Service intermediary 9
Article 18 System managers 9
Article 19 Service owners 9
Article 20 Information Security Officer 10
Article 21 Cyber and Information Security Centre 10
Article 22 Chief Information Security Officer 10

9. Section: Compliance 11
Article 23 Infringements and sanctions 11
Article 24 Improper analysis of logged data 11

10. Section: Final provisions 11
Article 25 Enactment 11

The Chief Information Security Officer of ETH Zurich

based on Art. 6 para. 4 (d and f) of the directive "Information Security at ETH Zurich"[1]

hereby decrees:

1. Section: General provisions

Article 1 Subject matter

[1] This directive governs the logging, analysis and monitoring of the system activities of IT resources and of system and user activities in the context of the use of IT resources at ETH Zurich.

[2] Logging refers to the recording of content as well as system and user activities.

Analysis refers to the targeted examination of recorded/logged data.

Monitoring is the systematic observation, recording or measurement of a procedure or process using technical aids, e.g. the monitoring of threshold values in order to intervene in a process if necessary.

IT resources[2] are all IT devices and IT services that are owned by or used on behalf of ETH Zurich. This also includes printers, scanners, software, telephony, building technology systems, building automation and outsourced services such as external cloud services. Video surveillance pursuant to Art. 36i of the ETH Act is excluded.

Article 2 Applicability

[1] This directive applies to all IT resources managed by ETH Zurich or managed on behalf of ETH Zurich and concerns any person who manages or analyses such IT resources or commissions or authorises their management or analysis.

[2] The logging, analysis and monitoring of IT resources in outsourcing, such as the connection of external cloud services, must be regulated separately by contract with the outsourcing provider or with the provider of external cloud services in accordance with this directive.

[1] RSETHZ 203.25

[2] Federal terminology: "electronic infrastructure"

Article 3 Goal and purpose

[1] This directive regulates the detection, prevention and tracking of security-relevant and operational events by logging and analysing data as well as monitoring IT resources.

[2] The purpose of this directive is to prevent and manage security-relevant incidents, which violate the confidentiality, integrity and availability of ETH Zurich's information and which may subsequently cause potential damage to the university.

[3] Operational events impair stable, uninterrupted operation.

2. Section: Logging

Article 4 Proper logging

[1] When using IT resources, data may be logged for the following purposes[3]:

a. to maintain the security of information and services,
b. for the technical maintenance of the electronic infrastructure[4],
c. to monitor compliance with usage regulations, in particular the usage regulations for IT resources at ETH Zurich,
d. to track access to the electronic infrastructure,
e. to record the costs arising from the use of the electronic infrastructure,
f. for the management of working time: the data on staff working hours,
g. to ensure safety: the data on entering or leaving buildings and premises of federal bodies and on their whereabouts.

Article 5 Contents to be logged

[1] System and user activities as well as technical security statuses of the IT systems (including configuration) may be logged.

[2] When processing personal data by IT means, the creation, processing, storage, modification and deletion must be logged whenever technically possible. In the automated processing of personal data (generally without human intervention), whenever technically possible, at least the storage, modification, reading, disclosure, deletion and destruction must be logged[5].

[3] The log provides information on the type, date and time of processing, the identity of the person (or technical identity) who carried out the processing and, if applicable, the identity of the recipient of the data.

[4] For security-relevant purposes, the following is logged:

a. synchronised date and time stamp (incl. applicable time zone)
b. origin of the log data (application / service name)

---

[3] BOT Art. 14 and Art. 57l (b, c, d) Government and Administration Organisation Act (RVOG, SR **172.010**)

[4] ETH terminology: "IT resources"

[5] Art. 4 Data Protection Ordinance of 31 August 2022 (DPO; SR **235.11**)

c. activity / event / error type
d. user or object ID / source address (IP addresses, MAC address, host name)
e. target system of the action (data, system, resource)
f. indication of whether the action was successful or not

[5] The scope of existing logging for security-relevant purposes may only be changed in exceptional cases and with the written confirmation of the CISO.

[6] For operational purposes, the content to be recorded may be supplemented by the service owner of a system in compliance with the provisions of this directive. Service owners provide an IT service to the customer and are responsible for said service over its entire life cycle and scope of services.

3. Section: Analysis[6]

Article 6 Proper analysis

[1] Log data may be analysed in accordance with Art. 57m, 57n and 57o RVOG[7] as follows:

a. not personalised;
b. on a random basis, not personalised by name (pseudonymised) or
c. personalised by name.

[2] Other findings about the activities of persons must be avoided. If such analyses arise, the CISO must be informed and will decide on the next steps. This type of analysis is considered strictly confidential[8].

[3] Users have no right to have their log data analysed.

Article 7 Non-personalised analysis

[1] The non-personalised analysis of recorded data is permitted[9]:

a. to maintain the security of information and services;
b. for the technical maintenance of the electronic infrastructure;
c. to monitor compliance with usage regulations, in particular the usage regulations for IT resources at ETH Zurich[10];
d. to track access to the electronic infrastructure[11] or
e. to record the costs arising from the use of the electronic infrastructure.

---

[6] See Section 3 et seq. of the Ordinance on the Processing of Personal Data and Data of Legal Entities when Using the Federal Electronic Infrastructure (VBNIB; SR **172.010.442** German only)

[7] Government and Administration Organisation Act (RVOG, SR **172.010**)

[8] Art. 57m RVOG; when analysing data, observe professional, business and official secrecy pursuant to Art. 57 Personnel Ordinance ETH Domain (PVO-ETH; SR **172.220.113** German only)

[9] Art. 57m Government and Administration Organisation Act (RVOG; SR **172.010**)

[10] RSETHZ 203.21

[11] This analysis also includes checking the contractual use of software or software services (software asset management).

[2] It is also permissible:

a. for all data, including the content of electronic mail: to secure them (backups);

b. for data on staff working hours: for the management of working time;

c. for data on entering or leaving buildings and premises of the federal authorities and on their whereabouts: to ensure safety.

[3] An order from the CISO is not required for the non-personalised analysis of data.

Article 8 Non-nominal personalised analysis

[1] The non-nominal personalised (pseudonymised) analysis of recorded data is permitted on a random basis[12]:

a. to control the use of the electronic infrastructure or

b. to monitor the working hours of staff.

[2] The extraction (securing of data) or analysis of non-named personal records is carried out exclusively on the instructions of the CISO. The non-personalised analysis of data is carried out by order of the CISO[13].

Article 9 Nominal personalised analysis (by name)

[1] The personalised analysis of recorded data by name is permitted[14]:

a. to clarify a concrete suspicion of misuse of the electronic infrastructure and to penalise proven misuse;

b. to analyse and rectify faults in the electronic infrastructure and defend against specific threats to this infrastructure;

c. for the provision of required services;

d. for the recording and invoicing of services rendered or

e. to control individual working hours.

[2] Analyses in accordance with paragraph 1 (a) are only permitted:

a. exclusively on behalf of the CISO;

b. whereupon, depending on the severity of the abuse, a decision is usually made together with the direct supervisor and other persons responsible for the person concerned (e.g. HR counsellors, study delegates) as to whether the analysis to identify the person concerned is carried out immediately or only after repeated detection of abuse; or

c. at the request of a criminal authority, e.g. a public prosecutor's office and

d. will in any case only take place after the person concerned has been informed in writing of the suspected abuse[15].

[12] Art. 57n RVOG

[13] This does not apply to the usual personalised analyses, e.g. ETHIS or SAP.

[14] Art. 57o RVOG

[15] Art. 57o para. 2 RVOG.

[3] The extraction (seizure) of data for evidentiary purposes in accordance with para. 1 (a) is only permissible:

a. exclusively on behalf of the CISO;

b. if there is a concrete suspicion of criminal offences. The President of ETH Zurich decides whether to press charges against offending members of the teaching staff or employees of ETH Zurich.[16] Further personal analyses are the sole responsibility of the competent criminal authority or

c. at the request of a criminal authority, e.g. a public prosecutor's office, whereupon the CISO will review the proportionality of the release of the data.

[4] Urgently required immediate measures in accordance with para. 1 (a and b) may also be initiated by the IT operators, in particular by the Director of IT Services or the Head of IT Services of the respective organisational unit. Such measures must be submitted immediately to the CISO for approval.

4. Section: Technical monitoring

Article 10 Monitoring and scanning of vulnerabilities

[1] If IT resources of ETH Zurich are used or operated on its behalf, the following data may be collected (scanned) and evaluated for the purposes described in Art. 4, Art. 7, Art. 8 and Art. 9 in order to identify vulnerabilities:

a. data on the technical status of those IT resources, e.g. patch statuses, open ports, protocols used, operating system version, etc. and/or

b. the peripheral data on the use of those IT resources, e.g. which telephone connection, email or IP address etc. communicated when, for how long and with whom.

[2] Scanning for both operational and security-related purposes is permitted for the responsible bodies within their area of responsibility (in particular the responsible system managers, Cyber and Information Security Centre - CISEC).

5. Section: Storage and deletion

Article 11 Deletion periods

[1] Data in accordance with this directive must be deleted by the competent body at the latest after the retention period specified below, insofar as the purpose of the analysis requires this[17] (exception: bring your own device, BYOD):

a. for backups of all data, including the content of electronic mail, provided these are not taken over by the university archive: maximum **2 years**;

b. for data on the use of the electronic infrastructure in accordance with Art. 4, in particular also data on the technical condition of the IT resources and peripheral data (security-relevant events in accordance with Art. 3): maximum **2 years**;

[16] Art. 14 para. 2 Rules of Procedure of the Executive Board of 10 August 2004(RSETHZ 202.3 German only).

[17] Art. 4 Ordinance on the Processing of Personal Data and Data of Legal Entities when Using the Federal Electronic Infrastructure (VBNIB; SR **172.010.442** German only)

c. for data on staff working hours for the management of working time**:** a maximum of **5 years** and

d. for data on entering or leaving ETH Zurich buildings and rooms and on the time spent in them to ensure security: maximum **3 years**.

[2] Log data regarding personal data must be stored for at least **1 year**[18]. For personnel dossiers and medical personnel data, Art. 10 of the Personal Data Protection Ordinance of the ETH Domain[19] (personal dossier: retention period 10 years).

[3] Log data on operational events in accordance with Art. 3 and Art. 10 may be stored for a maximum of **180 days**.

Article 12 Analyses

[1] The deletion periods pursuant to Art. 11 do not apply to seized data and analysis results.

[2] Data that is evaluated may only be stored for as long as it is required. They shall be destroyed by the competent authorities no later than three months after completion of the analysis or after expiry of the retention periods pursuant to para. 1.

6. Section: Centralised storage in the CISEC log container

Article 13 Forwarding of log data

[1] Security-relevant log data must be transmitted to the CISEC upon request. The service owner transmits his/her log data unchanged and encrypted as real-time information via a suitable interface to the log container designated for this purpose by the CISEC. Forwarding takes place after consultation. The storage of log data at CISEC serves to identify potential security risks.

The service owner may store log data locally in accordance with this directive. Log data must always be supplied:

a. important applications or databases of actively managed personal data;

b. IT resources that support critical processes in accordance with ETH Zurich's risk management;

c. of IT resources with high or very high protection requirements[20]

[2] The CISEC notifies the Service Owner in the event of an interruption in transmission.

[3] The CISEC forwards information on identified security risks and specific security-relevant incidents to the responsible parties (e.g. system managers, service intermediaries).

[18] Art. 4 Data Protection Ordinance (DSV; SR **235.11**); Art. 9 Personal Data Protection Ordinance ETH Domain (PDV-ETH; SR **172.220.113.14** German only)

[19] Art. 10 Personal Data Protection Ordinance ETH Domain (PDV-ETH; SR **172.220.113.14** German only)

[20] Directive Taking Inventory and Classification RSTEHZ 203.28

7. Section: Security requirements

Article 14 Confidentiality

[1] Log data is classified at least as confidential.

[2] Security-relevant, personalised analyses are considered confidential unless they are classified as strictly confidential by the CISO.

[3] All access to log data and analyses is severely restricted:

a. Third parties involved are carefully selected, undergo a personal security check (PSP) as required and are obliged to maintain confidentiality (non-disclosure agreement).

b. Access to log data must be secured for persons as far as possible using currently applicable access protection mechanisms such as multi-factor authentication (MFA) or certificate-based authentication (SSH).

[4] Access to log data for operational analyses is restricted to ETH employees with administration roles.

[5] Access to the CISEC log container is restricted to CISEC employees and must be traceable. CISEC employees and authorised persons must undergo an extended personal security check (PSP).

[6] The ISO decides on the allocation of additional authorisations in his/her own area of responsibility. These must be reviewed periodically (annually or as required). Decisions must be documented in a comprehensible and audit-proof manner and can be reviewed by the CISO.

Article 15 Integrity

[1] Log data must be traceable, complete and unchanged in terms of content:

a. they may not be deleted or changed.

b. Logging must not be switched off.

c. Sufficient storage capacity must be made available so that no entries are lost or overwritten. A predefined reduction of log data can be carried out after consultation with the CISEC.

d. The chronological order of the log entries is correct: all systems rely on Network Time Protocol (NTP)-based time synchronisation.

[2] Changes to the logging must be documented.

[3] As the service owner of the log container, CISEC ensures that

a. that the data in the log container is stored securely, evaluated in accordance with regulations and deleted in a timely manner, and

b. the log sources, retention periods, analyses and deletions are documented.

Article 16 Availability

[1] The service owner continuously monitors the logging and provides log data from his/her IT resources. He/she ensures that

a. logging is configured and available in accordance with CISEC requirements;

b. delays in log deliveries to the CISEC log container are eliminated and

c. compliance with these regulations is not circumvented.

[2] After consultation with the CISEC, the maximum tolerable period of time during which logging may be suspended must be observed.

8. Section: Duties

Article 17 Service intermediaries

[1] Service intermediaries procure external IT services (e.g. cloud services) and make these services available to members and guests of ETH Zurich.

[2] Service intermediaries shall agree with an external cloud provider on the logging, analysis and monitoring in accordance with this directive.

Article 18 System managers

[1] System managers are responsible for an assigned IT resource or network zone.

[2] With reference to logging, analysis and monitoring: System managers

a. log the events on their IT resources;
b. make this log data available to the service owner or the CISEC upon request and
c. irretrievably delete their log data after the maximum retention period in accordance with section 5.
d. report any misuse or concrete suspicion of misuse immediately to the CISO.

[3] System managers are information owners of their log data.

Article 19 Service owners

[1] Service owners provide an IT service to customers and are responsible for said service over its entire life cycle and scope of services.

[2] With reference to logging, analysis and monitoring: Service owners

a. set up a suitable logging infrastructure for their environment.
b. record and "monitor" in accordance with the requirements of this directive
c. irretrievably delete their log data after the maximum retention period in accordance with section 5.
d. monitor and ensure the confidentiality, integrity and availability of their log data.
e. define the log data to be recorded in accordance with the requirements of the CISEC.
f. offer their log data to the CISEC in a suitable form or ensure this as service-providing instances together with the system managers.
g. only make their log data available to authorised persons.
h. carry out operationally relevant non-personalised analyses under own responsibility.
i. obtain the necessary authorisation from the CISO in the case of personalised or non-personalised analyses in accordance with section 3.
j. report any misuse or concrete suspicion of misuse immediately to the CISO.

[3] Service owners are the information owners of the log data.

Article 20 Information Security Officer

[1] The Information Security Officers (ISO) are the first point of contact and advice centre for all information security issues in their area of responsibility.

[2] With reference to access to log data: The ISO

a. decides on additional, necessary authorisations in their own area of responsibility;
b. documents the decisions regarding additional privileged access rights for its own area of responsibility and
c. periodically reviews decisions regarding the allocation of additional privileged access rights.

Article 21 Cyber and Information Security Centre

[1] On behalf of the CISO, the CISEC is responsible for the technical-operational handling of information security incidents throughout ETH Zurich and for checking IT resources for security deficiencies.

[2] With reference to logging, analysis and monitoring: The CISEC

a. is responsible for the centralised log management of security-relevant log data and the implementation of security-relevant analyses throughout ETH.
b. operates the central CISEC log container and monitors the receipt of log data.
c. guarantees the confidentiality, integrity and availability of the log data transmitted by the IT resources throughout the entire life cycle.
d. reports to the CISO any misuse or concrete suspicion of misuse identified on the basis of an analysis.

[3] The CISEC is the information owner of the centralised, security-relevant log data.

Article 22 Chief Information Security Officer

[1] The Chief Information Security Officer of ETH Zurich (CISO) is responsible for information security at ETH Zurich.

[2] With reference to logging, analysis and monitoring: The CISO

a. is the exclusive client of non-nominal and nominal personalised analyses;
b. decides on an extension of the retention of personalised and non-personalised analyses and the underlying log data;
c. may verify compliance with the provisions of this directive;
d. may impose measures and sanctions, in particular in the event that log data is not evaluated as intended.

[3] The CISO is the information owner of non-personalised analyses and the underlying log data.

9. Section: Compliance

Article 23 Infringements and sanctions

Based on an analysis of data, the CISO may order protective and precautionary measures or sanctions in accordance with Section 4 of the Regulations on the Use of IT Resources at ETH Zurich .

Article 24 Improper analysis of logged data

[1] The CISO may check or have checked compliance with the provisions of this directive.

[2] If log data is not evaluated as intended, the CISO may impose the following measures and sanctions:

a. Warning and, in the event of a repeat offence, forwarding to the legal department / VPPL / rectorate or other responsible body for further action
b. the precautionary blocking of access to the log servers
c. the blocking/backup of data for evidence purposes.

[3] The wilful or repeated improper analysis of log data is considered serious misuse and may result in disciplinary or personnel-related measures.

[4] Knowledge of serious misuse within the meaning of paragraph 3 requires reporting to the CISO.

10. Section: Final provisions

Article 25 Enactment

This directive enters into force on 01 January 2025. Article 5 paragraph 2 (Logging of personal data) is verifiable from 01 January 2027.

Zurich, 1 January 2025

Johannes Hadodo
Chief Information Security Officer
ETH Zurich