enisa

European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

IT MANAGEMENT & ADMINISTRATION

Record of processing activity	
Title	IT management & administration
Name and contact details of controller	ENISA, Corporate Support Services (IT), it-helpdesk@enisa.europa.eu
Name and contact details of DPO	dataprotection@enisa.europa.eu
Name and contact details of Joint Controller	European Commission, DG DIGIT is a controller with regard to the ECAS account (EU login) that provides access to the Commission’s internal systems that are available for ENISA’s staff. The ENISA ISO is a joint controller in the case of Splunk monitoring tool for security alerts provided from European Commission CERT-EU as a service.
Name and contact details of processor	ENISA contractors involved in the maintenance of ENISA IT systems and services; European Commission CERT-EU in the specific case of the Splunk platform (provided as a service).
Purpose of the processing	To support various standard IT management processes that are required for ENISA's operation (e.g. access to various systems/tools/services, corporate email management, device management); To support the security of ENISA's networks and systems (through the operation of standard network and system monitoring tools).
Description of data subjects	All ENISA staff, including statutory staff, interims, trainees and SNEs.
Description of data categories	Data associated with user management and administration within different internal ENISA IT systems, i.e. user account information (name, username, position/department/unit) and associated access rights, device IDs associated to ENISA users (staff members), troubleshooting issues referred to IT by ENISA users (via ticketing system on ENISA's intranet), etc. Data associated with user management in European Commission's systems through ECAS system (EU login), i.e. username, employee number, name, date of birth, email, type of contract and activity status. Data associated with standard network and system monitoring and logging processes, such as IP addresses, and traffic data, which might be included in system logs, incident/event logs, spam/malware filtering or other relevant processes. Note that such processing is performed automatically by technical tools and IT staff will only access relevant data in ad hoc cases of troubleshooting or investigation of security events/incidents.
Time limits (for the erasure of data)	User account and relevant access information to ENISA's IT systems are kept as long as ENISA staff are active and using the relevant systems. ECAS related data are kept as long as the ENISA staff are recorded as active users by the European Commission and for a period of one year thereafter. Specific retention periods apply to different systems and processes (e.g. email policy, acceptable use policy, device management policy, etc.). Specific systems retain data for no longer than the period required in order to ensure business continuity in compliance with the applicable retention periods.

Data recipients	Designated ENISA IT staff, designated staff of the European Commission (for ECAS account only), designated staff of the ENISA processors, as well as the ENISA Information Security Officer, exclusively for the purpose of IT management and administration.
Transfers to third countries	N/A
Security measures - General description	General security policy and relevant technical and organisational measures of ENISA internal IT system. Security policy of EC with regard to ECAS account management.
Privacy statement	Published in ENISA's intranet for all staff.