



Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		

Version history

Version	Version date	Version update	Change description
01	10/06/20	Creation	


Players in this version

Date	Role	Position	Person
10/06/20	Assistant author	IT Manager	BOULOGNE Pascal
10/06/20	Main author	IT Manager	BOULOGNE Pascal
10/06/20	Assistant proof reader	Quality Project Manager	GEORGEL Anne
10/06/20	Main proof reader	Quality Project Manager	GEORGEL Anne
10/06/20	Approver	Maintenance Sector Manager	FAVROLLE Stephane

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

CONTENTS

1	<u>REFERENCE DOCUMENTS</u>	3
2	<u>REFERENCE STANDARDS</u>	3
3	<u>GLOSSARY/DEFINITION</u>	3
4	<u>PURPOSE</u>	3
5	<u>PROCESSES COVERED</u>	4
6	<u>ROLES AND RESPONSIBILITIES</u>	4
7	<u>DESCRIPTION</u>	5
8	<u>REVIEW</u>	15
9	<u>ATTACHMENTS/EXTERNAL LINKS</u>	15
10	<u>APPENDICES</u>	15

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

1 REFERENCE DOCUMENTS

ADK-USINE-ELT10-PDG-0001:	Operational control
ADK-USINE-ELT1-MSI-0001:	Integrated System Manual
ADK-USINE-ELT1-POL-0001:	Policy
ADK-USINE-ELT8-PDG-0001:	Document, data and record management

ADK-MAC-ELT10-POP-0013:	POP Computer hardware and electric equipment recycling
ADK-MAC-ELT10-POP-0022:	POP Subcontractor information system access policy

ADK-USINE-ELT5-ENR-0001:	Operational line role matrix
ADK-USINE-ELT5-ENR-0002:	HS2EQ role matrix

2 REFERENCE STANDARDS


Element 10	Operational control
IATF 16949 - 8.1	Operational planning and control
ISO 14001 - 8.1	Operational planning and control
ISO 50001 - 8 Conducting operational activities	
ISO 9001 - 8.1	Operational planning and control

3 GLOSSARY/DEFINITION

4 PURPOSE

4.1 Purpose of the document

This document sets out the conditions for the implementation of the company *information systems security policy* (ISSP); it defines the objectives to be met and the resources assigned to meet them. It reflects senior management's strategic vision of IS security and is based on the ISO 27002 standard.

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		

4.2 Scope of application

The ISSP applies to all company *information systems* (IS).

The ISSP concerns all persons involved in the IS, including company staff and subcontractors (External Contractors)

Most of the ISSP security rules are basic rules defined by the ANSSI (Agence Nationale de Sécurité des Systèmes d'Information)


5 PROCESSES COVERED

MASUPMA	Maintenance Support Maintenance, IT-Automation, Asset Management CMX Reliability and Regulatory Control
---------	---

6 ROLES AND RESPONSIBILITIES

Position	Role	Responsibility	Authority

This table supplements the position role descriptions for the above roles in the Element 5 plant EDM and the ADK-USINE-ELT5-ENR-0001 and 0002 matrices.

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

7 DESCRIPTION

1. Context

ISSP management

The ISSP can change over time to take into account changes in security rules, changes in threats and changes in organisational, legal, regulatory and technological contexts. It is reviewed at the very least every year.

These changes are monitored by the CISO (on our production site, the IT manager acts as CISO) in liaison with management; the CISO's main missions are:


- Monitoring ISSP implementation
- Suggesting updates
- Monitoring technical developments
- Facilitating implementation

ISSP Implementation

The IT department draws up an inventory of its information systems, conducts risk analyses and implements appropriate continuity measures, conducts IS security awareness and training actions, conducts security level checking actions, and implements a process used to deal with security alerts and incidents.

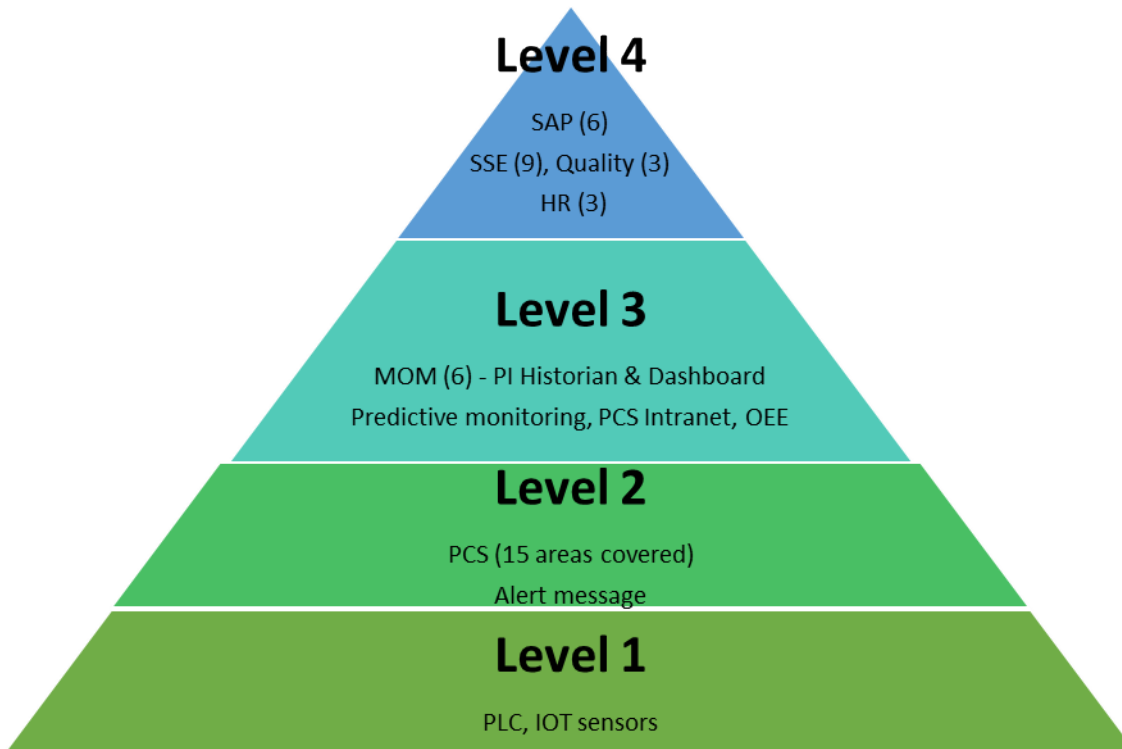
Incident processing and crisis management

If an attack occurs, the players involved require increased monitoring and coordination; every IS sector and player must report any event that impacts or could impact the availability, integrity, confidentiality or traceability of the IS to the CISO. A GLPI **security** type ticket must be created for each event. An ISS emergency situation is the result of any alert or incident on one or more IS systems causing a major malfunction in the company's activities; such situations will be managed by the site crisis unit and will also be the subject of a security ticket. Feedback on the handling of these attacks will be attached to the ticket.

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

2. ISS scope


IS security covers all the production site information systems from level 1 to level 4 (ISA-S95 standard for industrial companies)



Level 4 contains all the management and office applications
Level 3 contains all the industrial applications (workshop management)
Level 2 contains all the industrial workshop control applications
Level 1 contains all the workshop process automation equipment and applications

These levels are based on common infrastructure layers: networks (internal and external), servers, operating systems, workstations, etc.

Added to that are the company's communication tools which can be fully or partially reliant on those same infrastructure layers: VoIP, video-conferencing, video surveillance, access control, walkie-talkie, etc.

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	Version: 01
Publication date: 10/06/20		

3. Security needs

IS security is based on the following criteria:

Confidentiality: "Confidentiality is the property that information is not made available or disclosed to unauthorised persons, entities or processes" - ISO 7498-2 (ISO90) standard.

- *Availability*: The guarantee that the information or service is accessible when required by authorised persons.

- *Integrity/Accuracy*: "Integrity is the property that data has not been altered or destroyed in an unauthorised manner" ISO 7498-2 (ISO90) standard. The guarantee that the data is accurate and complete.

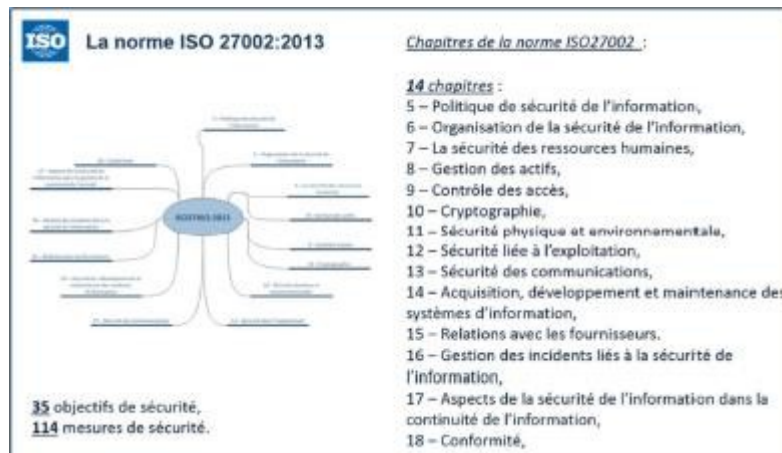
- *Integrity/Proof*: The guarantee that actions are traced so that proof can be produced

Security requirements apply both to IS resources (workstations, networks, applications) and to the data processed by those resources. Such data must be inventoried and even classified to identify the degree of sensitivity and, consequently, the need for protection.

An audit was conducted in April 2019 (based on ANSSI hygiene rules), and is the roadmap presented to senior management to secure the Information System.


4. Document management

This document defines a list of IS security objectives and best practices.



For ease of reading, each of the 14 sections includes a reference to the standard (ISO5x). Each section is organised as follows:

- Section title corresponding to the relevant section of the standard
- Existing safety measures
- Future actions, if any

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

5. Information security policies (ISO§6)

Objective: To set up an organisation that guarantees that security is taken into account both preventively and responsively

5.1 *Internal organisation*

5.1.1. *ORGASECU-6-1-1: IS governance*

The CISO validates the ISSP application measures (coordinates and plans the actions) and updates the application documents within his/her remit. He/she uses security information from his/her partners and CERT alert and watch bulletins. He/she distributes the site electronic resource use charter to staff. He/she proposes and implements user awareness-raising actions covering IS security issues.

5.1.2 *ORGASECU-6.1.2: IS and project management*


All new systems must undergo a security analysis to identify the threats that could impact system operation, and the appropriate security rules must be applied. This analysis is conducted by the CISO alongside the functional project manager.

5.2 *Mobile devices and teleworking*

The site authorises email access for all staff who have an account in the company directory. To this end, a procedure has been distributed to staff making it possible for them to install the company messaging system on any personal device that complies with the company security rules ("*Access to the company messaging system from a personal smartphone*" procedure)

Teleworking can be authorised in the following conditions:

- Request made to the IT department
- Requester holder of an encrypted company laptop and a VPN setup token, or requesters who have access to the Citrix web portal (secured by double authentication) from a personal device

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		

6. Human resource security (ISO§7)

Objective: To make users the strong links in the company IS. The provision of IT resources must be formalised on the arrival, change of position, or departure of users.

6.1 SECUPERS-7-1: Personnel management

Security checks are proportionate to business requirements and risks identified during the recruitment interview. Human resources informs new arrivals at the site of the company by-laws and the IT charter (induction booklet); non-permanent staff (interns, temporary staff, external contractors, etc.) are informed of their duties when they are given access by the on-site Help Desk (issue of the IT charter). Access is issued following a request using the IT access request application. The new arrival management procedure ("*user management*" procedure) is used to assign the standard resources they will need (hardware, messaging, application access, etc.). The same procedure will be used for changes of position and departures from the company.

6.2 SECUPERS-7-2: Awareness raising

The CISO regularly communicates on IS security risks and best practices via messaging, lecture hall or video. Users must be trained in the use of the work tools.

7. Asset management (ISO§8)

Objective: To identify company assets and define the appropriate data protection responsibilities.

7.1 GESTACTI-8-1: Technology inventory and control

There is an up-to-date list of assets which is stored in the asset and ticket management software (GLPI). The Infrastructure manager is in charge of asset management. Risk analyses are used to identify application and data criticality.


7.2 GESTACTI-8-2: IS map

There is an application map and logical and physical architecture diagrams that make it possible to view and locate the Information System technical and application components.

7.3 GESTACTI-8-3: Data classification

The business units conducted a risk assessment (in 2010) to classify data in terms of availability. That assessment must be renewed, and an integrity and confidentiality classification added. Data likely to contain personal information is identified in the GDPR map maintained and updated by the site security officer.

7.4 GESTACTI-8-4: Hardware recycling

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		

Appropriate skips are provided for the recycling of electronic equipment; hardware is systematically mastered before being handed over to a new user to guarantee that the data is erased (a procedure governs the recycling process - MAC-ELT10-POP-0013-04)

8. Logical accesses (ISO§9)

Objective: To control user access and prevent unauthorised access to the IS

8.1 ACCESLOG-9-1: Network access

Network access is provided by the Sharepoint "Access request" application (see "user management" procedure). The persons authorised to grant access are the site administrators. The rights granted are requested by the HR department or the principal for external companies.

A monthly audit procedure requires that any account that has been inactive for more than 90 days be deactivated.

8.2 ACCESLOG-9-2: Nominal network access accounts

There is a password management policy. This policy especially describes the number of characters, the complexity and the change frequency based on ANSSI standards, the definition can be found in the electronic resource access charter (General access and security)

The charter reminds users that they are responsible for the use of their account and password and must not disclose them except for service reasons validated by the user's sector manager.

8.3 ACCESLOG-9-3: Generic network access accounts

Generic accounts are used to open work sessions in the workshops (business office) automatically (pre-configured workstation). The password complies with the above policy.

8.4 ACCESLOG-9-4: Authorisation management


Authorisations are issued based on business functions; all access requests are validated by a line or functional manager - the access request application will be used for this purpose. An authorisation audit is conducted quarterly using the NETWRIX tool.

8.5 ACCESLOG-9-5: Privileged accounts

An audit is conducted quarterly using the NETWRIX tool on the use of high privilege accounts (administrator account); restricted accounts reserved for specific tasks (email, workstation) exist.

8.6 ACCESLOG-9-6: Service provider accounts

The organisation authorises service provider partners to have network accounts; these are audited in the same way as the organisation accounts (to differentiate them, such accounts have an end date (of the contract), their company name in the Organisation/Company field, and their principal is indicated in the Organisation/Manager field); service provider partners working on site are created in the USERS organisational unit in the same way as the organisation's staff; support service provider partners not working on site are created in the USERS\External organisational unit.

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		

9. Logical access (ISO§10)

Objective: To guarantee the correct use of encryption to guarantee data confidentiality, authenticity and integrity

There is an in-house certification authority to validate access to applications requiring it; certain site sectors may also use this authority to guarantee the authenticity of their emails.

All Internet applications that use personal data will be encrypted (external certificate inventoried by the site)

10. Physical security (ISO§11)

Objective: To prevent all unauthorised physical access, intrusion / damage to data; to prevent the loss or theft of assets that could lead to the interruption of company activity

10.1 SECUPHY-11-1: Physical access control to computer rooms

Access to the rooms is restricted (rooms equipped with a physical access control system); permanent staff are listed in the computer room access procedure which is revised annually.

10.2 SECUPHY-11-2: Premise fire protection

A fire detection system is managed by central maintenance; this system protects the computer rooms.

10.3 SECUPHY-11-3: Essential services

Services essential to IS assets are the supply of energy and cooling. All the rooms are equipped with a UPS (the two main rooms have UPS with a 5-hour autonomy) and air conditioning. This equipment is managed by the site's central maintenance department.

11. Operational security (ISO§12)


Objective: To guarantee secure operations in accordance with IT practices. To guarantee that data is protected, that are events recorded, and that the integrity of operating systems is also guaranteed

11.1 SECUEXPLO-12-1: Operating procedures

The main operating procedures are updated in the IT Documentary Teams (a folder is reserved for security)

11.2 SECUEXPLO-12-2: Malicious software

An antivirus solution is deployed on all workstations connected to the company IT network. Messaging is protected by a third-party solution. Internet browsing flows are protected by filtering the browsed websites (website category, filtering of high-risk sites), IPS (Intrusion Prevention System) and application filtering using double firewalls.

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

11.3 SECUEXPLO-12-3: Workstation security

Workstations are protected as follows:

- System and application patches are deployed before the workstation is delivered
- An antivirus is installed
- Hard disk encryption is used for laptops (users with a VPN solution)
- No users are the administrators of their workstation, privilege escalation is disabled

11.4 SECUEXPLO-12-4: Data backup

Network workspaces are made available to users (a personal workspace (synchronised off-line for laptops) as well as collaborative workspaces - they all are backed up (two-hour restore point); the servers are backed up at different frequencies depending on the criticality of the hosted applications. Physical and virtual machine procedures detail the types of data backed up, the media used, the backup frequency and timeslots and their retention period. Documented annual restoration tests are carried out.

11.5 SECUEXPLO-12-5: Vulnerability management

All workstations and servers are updated regularly (monthly for workstations) using Microsoft's WSUS patch distribution service. For critical security alerts, all the workstations are updated immediately.

11.6 SECUEXPLO-12-6: Installation of software, hardware and connection of mobile devices


Software and hardware is installed by the IT support team, as users do not have the required privileges. Removable media are authorised for a limited population (rights managed by the antivirus console) The deployment of smartphones and tablets is managed using Microsoft's Intune management solution to guarantee compliance for all devices with access to company data. Users are not administrators of their own workstations.

11.7 SECUEXPLO-12-7: Activity logging

All operations on the company directory, VPN and Internet are kept for 1 year in accordance with current regulations. Domain authentication logs are also accessible and usable.

11.8 SECUEXPLO-12-8: User remote support

Users can receive remote support via a remote control tool. All access to the workstation is subject to the user's authorisation.

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

12. Communications security (ISO§13)

Objective: To guarantee the protection of data on networks

12.1 SECUCOMM-13-1: Network control

Network access is subject to authentication by login and password on the wired network and by an additional certificate on the wireless network (radius solution, deployment of WPA2 AES (encryption) & 802.1X (user authentication) & PEAP (certificate) security on portable workstations)

The network architecture is designed to meet all availability (two unified main rooms, double attached remote rooms, supervised hardware), confidentiality and integrity requirements.

VLAN management is available, as well as a "demilitarised zone" (DMZ) for hardware accessible from the outside.

There are several WIFIs:

- Guest: captive, partitioned portal only providing Internet access (logs saved)
- Smartphone and PC (ADKWIFI): secure access by authentication (level 4)
- DECT phone (ADKVOIP): secure access (Company WPA2)
- Production (PLC): secure access (WPA) - (level 1)

Internet accesses are filtered.

12.2 SECUCOMM-13-2: Operators


Access to the Internet network and remote websites is provided by routers connected using very high-speed optical fibre (SDSL solution on backup site)

12.3 SECUCOMM-13-3: Messaging and other exchange channels

The site uses the Office 365 solution for the messaging tool and rolled out the following features to users in 2019:

- Collaborative work: Sharepoint and Teams
- Document sharing: Sharepoint and OneDrive
- Instant messaging: Teams and Cisco Jabber

Communication tools are connected to the company directory. For external accesses, two-factor authentication is required (Microsoft MFA for access to the Citrix Web portal and Fortinet MFA for IPSEC VPN from a company computer)

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

13. Acquisition, development and maintenance (ISO§14)

Objective: To guarantee that information security is an integral part of Information Systems throughout their lifecycle

13.1 DEVMAINT-14-1: Analysis and specifications

Security requirements must feature in the specifications in the form of architecture diagrams validated by the network administrator, availability assessments (downgraded mode), access methods, etc.

13.2 DEVMAINT-14-2: Remote maintenance

As part of their contract, service providers may carry out remote maintenance operations (in compliance with the MAC-ELT10-POP-0022 procedure) using a VPN or temporary access using a Citrix portal.

14. Relations with service providers (ISO§15)

Objective: To guarantee the protection of the organisation assets accessible to external contractors

14.1 RELPREST-15-1: Data security with our service providers

The security charter must be issued to the service provider when the access account is provided.

14.2 RELPREST-15-2: Data security in agreements

The security requirements are defined in the policy, which will be communicated for all new agreements with an external partner.

14.3 RELPREST-15-3: Monitoring and review

The IT department regularly monitors and reviews accesses granted to external staff. A decision may be made to withdraw access if breaches occur.

15. Incident management (ISO§16)


Objective: To guarantee an information security incident management method including event communication

15.1 GESTINCI-16-1: IS security incident reporting

All security incidents are reported to the CISO for entry into the incident management tool.

15.2 GESTINCI-16-2: IS security incident processing

All events that could have an impact on IS security (availability, integrity and confidentiality) are processed by the system administrators in collaboration with the CISO.

Central maintenance	ADK-MAC-ELT10-POP-0024	
Creation date: 10/06/20	POP Information System Security Policy IT/NT041	
Publication date: 10/06/20		Version: 01

16. Business continuity management (ISO§17)

Objective: Data security continuity is part and parcel of IS continuity

16.1 GESTCONT-17-1: Data security continuity organisation

The site must identify the threat scenarios, which it protects against and counters, using a continuity plan.

17. Compliance (ISO§18)

Objective: to avoid all breaches of legal or contractual obligations relating to data security and to avoid all breaches of security requirements

17.1 CONFORMI-18-1: Privacy and GDPR

The site has begun the process of upgrading to compliance with the GDPR. A DPO has been appointed and has implemented:

- A personal data processing register
- Personal data mapping

17.2 CONFORMI-18-2: ISSP compliance

The CISO conducts or commissions audits to check that the rules are being applied correctly, and conducts or commissions penetration tests to make sure the IS is secure and to make progress in implementing new barriers.

17.3 CONFORMI-18-3: Audit management

The CISO takes into account audit results and modifies the ISSP accordingly.

8 REVIEW

This document must be reviewed at least every 3 years et revised (change of version) when necessary, especially when there are requirements or changes following an audit or an incident.

9 ATTACHMENTS/EXTERNAL LINKS

--	--	--

10 APPENDICES