

## DESCRIPTION OF THE SECURITY FEATURES OF THE 'SECURE ROOM'

### A. Physical infrastructure and logistics of the secure room

The secure room will be designed and built in full compliance with Commission Decision (EU, Euratom) 2015/444, which lays down security rules for the protection of EU *Classified Information* (EUCI) intended for European institutions. This decision defines strict procedures for the management, handling and protection of classified information, including classification levels, authorisation criteria and technical and organisational measures to be adopted.

The room, which will be large enough to accommodate all the equipment needed for handling EUCI, will be constructed with reinforced walls, floor and ceiling in accordance with standards approved by the European Union Security Authority (EUSA) or equivalent body. This includes certified anti-intrusion materials, sound insulation systems and shielding against electromagnetic interception (TEMPEST).

Access will be strictly controlled using multimodal security systems: electronic badges, advanced biometric systems (e.g. facial recognition or fingerprints), with an electronic register accessible only to authorised personnel. Both badges and credentials will be subject to strict management in accordance with European protocols for secure access management.

The room will be equipped with highly sensitive intrusion detection systems, high-resolution video surveillance compliant with GSA (General Services Administration) standards, and integrated anti-intrusion alarm systems connected to a 24/7 security centre. There will also be state-of-the-art fire protection systems, with environmental sensors to monitor temperature, humidity, and other critical parameters that could affect physical security and information integrity.

Unauthorised communication devices, such as mobile phones or wireless devices, will be strictly prohibited, while secure terminals compliant with European encrypted communication standards will be used for operational purposes.

All keys and access credentials will be managed using certified procedures, ensuring complete traceability and accountability for each operator, as required by the European Commission's guidelines for the management of classified materials.

The entire infrastructure will also comply with best practices relating to physical and IT security outlined by agencies such as the *European Union Agency for Cybersecurity* (ENISA) and will be subject to periodic security checks, independent audits and ongoing risk assessments.

In summary, the secure room will offer a protected environment that guarantees the confidentiality, integrity and availability of EUCI information, ensuring compliance with the most up-to-date European Decisions/Directives in the field of classified information security, with a view to continuous protection and resilience against internal and external threats.

## **B. IT features of the secure room**

In order to ensure compliance with international information security standards and to safeguard the confidentiality of activities carried out in the “secure room”, the site will be equipped with advanced technological measures, as outlined below. These measures will be integrated into the Information Security Management System (ISMS) in compliance with ISO/IEC 27001 and relevant national guidelines on the protection of critical infrastructures.

- Network isolation: implementation of air-gapped architectures, with no direct connections to the Internet or insecure corporate networks, and dedicated segmentation for EUCA activities; strong authentication and end-to-end encryption (TLS 1.3, IPSec). All connections to external domains outside the secure room will be allowed exclusively through dedicated security gateways, properly filtered, encrypted, and monitored, in order to maintain a strict logical isolation model.
- Protection against environmental eavesdropping: electromagnetic shielding of walls, soundproofing to prevent acoustic leaks, shatterproof and anti-intrusion windows; reinforced doors with dual access control verification (badge plus biometric factor).
- WIFI Management: preference for wired connections, preferably fibre optic; only if strictly necessary, use of Wi-Fi with WPA3 standard, 802.1X authentication, hidden SSID, and VLAN segmentation. Wi-Fi usage will be limited to strictly operational needs, with continuous monitoring of emissions and active connections.
- Autonomous power supply: UPS systems and generators to ensure operational continuity, with capacity designed for at least 72 hours in the event of a prolonged power outage.
- Monitoring and logging: SIEM systems for anomaly detection and secure event logging, with retention of security logs for a minimum period of 12 months, in line with best practices and obligations under European regulations (e.g., NIS2).
- Dedicated encrypted communications: protected channels for exchanging sensitive information, based on encrypted protocols with strong cryptographic resistance (e.g., TLS 1.3 with Perfect Forward Secrecy) and mutual authentication mechanisms.
- Infrastructure redundancy: backup lines for network and power, and critical devices configured for high availability (e.g., active/active or active/passive clusters) to minimize the risk of a single point of failure.
- Advanced environmental control: sensors for temperature, humidity, fire detection, and intrusions, connected to a centralized supervision system that triggers alarms and predefined response procedures.

- Centralized governance: dashboard for real-time access and configuration management, with operator profiling, tracking of administrative activities, and periodic review of privileges.
- Policies and organizational controls: access to the secure room is allowed only to pre-authorized personnel, with registration of entries/exits, a ban on personal devices (BYOD), controlled management of removable media, and periodic audits of configurations and logs.

The implementation of the described measures ensures high levels of protection against both physical and logical threats, preventing unauthorized access, information leaks, and physical and cyber compromises in high-risk scenarios.