SECURITY STANDARDS

The Supplier must follow all relevant security requirements:

- Strict, well-defined, and documented security policies and procedures.
- Ensure annual security awareness training for your involved employees.
- The security controls in place to appropriately protect the confidentiality, integrity, and availability of the FEG information assets and systems, and their efficiency is confirmed by regular testing.
- Enable to follow security requirements from ISO27001 standard.
- Enable to run independent security audits and assessments.
- Follow need-to-know, least privilege and segregation of duties principles.
- Reporting any rule violations and/or security incidents.
- Ensure cooperation during investigation of potential security incidents.
- Enable logging and access to logs.
- Enable appropriate authentication (integration with Active Directory) and authorization mechanism.
- Ensure functional Vulnerability and Patch management.
- Enable integration of delivered solution with Identity and Access Management (IdM) tool.
- Enable exit procedure.
- Ensure compliance with requirements also from your vendor and/or subcontractor, to whom provides access.
- FEG Security clauses as part of future contract.