FRANCE

Reference : IT_EFR_001_V13_EN_SECURITY PRINCIPLES

EQUANS France – Information Systems Department

Security Principles

Applicable since 15/04/2024

	AUTHOR	VERIFIER	APPROVER	DIFFUSION
Role	RSSI assistant	M-BISO BU France / L-CISO BU France	M-CISO BU FRANCE	For EQUANS and its entities
Name	CYBER Team	Jérôme ARHUIS Ronan LAGATHU Guillaume VACHER	Suvansh LAL	

OBJECTIVE : This document specifies the implementation modalities at EQUANS France and its entities of the security and resilience principles derived from EQUANS Group's security policies.

SCOPE : The principles stated in this document apply to all departments, professions, and entities of EQUANS France.

Indice	Date	Mises à jour apportées
01	21/03/2025	Creation
10	18/04/2024	Approval
11	31/03/2025	Intégration of Client IS
12	16/04/2025	Validation of the version 13

TABLE DES MATIÈRES

1. INTRODUCTION ET PRINCIPES GÉNÉRAUX

A. General Definitions

The definitions provided below apply to the entire document:

- **Company**: EQUANS France;
- **Group:** EQUANS Group;
- **User:** Any individual (employee, apprentice, intern, temporary worker, contractor), regardless of their access location, having an account that grants access to the Company's Information System (IS);
- **Client:** External entity having a contractual relationship with Equans or one of its affiliated entities for which services are performed. These services use digital products or services to support activities carried out by Equans employees, affiliated entities, and/or their subcontractors.
- **CORPORATE IT**: All computer and telecommunications resources, hardware or software, that the Company provides to Users for professional purposes;
- **CLIENT IT**: All computer and industrial resources, hardware or software, provided by the Company or the Client, used by the Group's businesses in the context of integration, maintenance, operation, supervision, and development activities.

B. Preface

Within a general context of evolving cybersecurity threats and strengthening of the legal and regulatory framework (e.g., Military Programming Law, National Security Directive, GDPR, Cyber Resilience Act, European Directives...), the Company is a stakeholder in the security of the CORPORATE IT Information System and the framework of the security level of CLIENT IT Information Systems, under the governance of the M-CISO France.

This document specifies the Company's security principles that enable achieving its objectives on the security of CORPORATE IT and CLIENT IT Information Systems:

- Compliance with legal and regulatory obligations;
- Duty of advice;
- Internal audit;
- Protection of its infrastructures (IS) and its application services;
- Protection of its data and that of its clients.

These principles are based on the requirements contained in the Group's security policies, accompanied by specific measures contextualized by business activity.

C. Documentary Corpus

Management Commitment Letter: positions the importance of information security within the Company.

- **CORPORATE IT IS Security Policy (IS Security Policy)**: contains the general principles regarding IS security, responsibilities, and organization, including technical security measures applicable to **CORPORATE IT IS**.
- **CLIENT IT IS Security Policy ISSP** : contains the general principles regarding the Group's IS security and specific governance adapted to the client context, including technical and organizational security measures applicable to the dedicated **CLIENT IT IS** under contract.
- **CLIENT IT IS Operational Security Policy ISSP-O:** Policy grouping technical and organizational measures by business domain or technical domain. They reflect the best practices of ANSSI and/or standards such as ISO 27002:2022 or IEC 62443.
- **Security Principles (this document):** based on the ISO 27002:2022 standard, presents the security measures in place in a synthetic manner, with documentary references to obtain implementation details (Group domain policy, specific policy or procedure of the Company...).
- **Specific policies and procedures**: these documents provide measures specific to the Company in relation to the Group's domain policies. The measures must comply with those of the Group. For example, a legal or regulatory constraint specific to France may reinforce a Group security measure. They are classified into two categories, CORPORATE IT for internal use and CLIENT IT: contextualized to the activities carried out by the Group's businesses for the benefit of their Client.
- **Charters**: charter for the use of the Company's IT resources, administrator charter, integrated into the internal regulations of the Group's legal entities.
- **The 10 Golden Rules of Cybersecurity:** 10 best practices in cybersecurity.
- **Statement of Applicability (SoA):** security measures from Annex A of the ISO 27001:2022 standard with, for those retained, the documentary references for their implementation.
- Documents concerning the Company are available on the Intranet "Ref'IT". Documents concerning the Group are available on the Intranet "GRC EQUANS - Cybersecurity".

D. Document Distribution

This document is accessible to all Users of the Company and its entities, online on the Intranet. Furthermore, it is intended to be distributed outside the Company, for example, to accompany a response to a call for tender or a contract. Other documents in the Company's and Group's IS Security documentary corpus are not intended for wide distribution. They can be consulted on-site or provided to auditors with the prior agreement of the Company's CISO.

E. Scope of Application

This document aims to present the unified CYBER governance of Equans France.

It is constituted as a summary:

- of the IS, whether or not hosted by a third party;
- of the IS Users (employees, external third parties...);

- of the entities and BUs attached to the Company: these are the General Management and the managerial lines of the Company and the attached entities that bear the responsibility for implementing security requirements.

It is the responsibility of the Company to ensure the implementation of security requirements, even if their operational deployment is handled by a third party (for example, in the case of Cloud hosting).

2. SECURITY PRINCIPLES - COMMON PRINCIPLES

A. Organization

The Executive Committee of Equans France has designated the Information Systems Department and its Cybersecurity Department responsible for applying the Group's CYBERSECURITY strategy. In this context, the security of CORPORATE IT and CLIENT IT information systems is placed under the governance established by the M-CISO (CISO) of Equans France.

The Cybersecurity Department of the Information Systems Department of Equans France is organized into 5 units:

- **Governance risk compliance** - Risk management, compliance with procedures and policies
- **Security operations** - Monitoring of technical vulnerabilities and remediation
- **Security project office** - Management of security integration in projects
- **Digital resiliency** - Management of operational resilience of CORPORATE IT
- **Cyber customer trust** - Risk management, Audit, and Advisory on CLIENT IT

They rely on the Cybersecurity Departments of Equans CORP:

- **Cyber technical office** - Governance body of the Equans Group
- **SLS cyberdefense - soc/cert/csirt** service center
- **SLS cyber customer trust** - CCT service center

The DSI departments deploy the security measures of their scope; they support and assist the Cybersecurity department on CORPORATE IT.

The business divisions of Equans France organize business operations on behalf of their Clients. They ensure the consistency of operational responses carried out by the legal entities holding the contracts. In this context, they may carry out integration, maintenance, operation, supervision, and development activities for the benefit of their Client. The framework of the security level on CLIENT IT is managed by the M-BISO of Equans France through the CYBER CUSTOMER TRUST FRANCE program.

Users of the Company's CORPORATE IS comply with the requirements of the CORPORATE IT IS Security Policy and the Charter for the use of IT resources.

Users of CLIENT IT comply with the requirements specific to their business contexts. In this context, the cybersecurity requirements to be considered are explicitly mentioned in the contract of the business, as contractual clauses and/or Security Assurance Plan. They can be detailed, if necessary, within a CLIENT IT IS Security Policy.

The CYBER CUSTOMER TRUST FRANCE program is responsible for managing the level of cybersecurity risk by acting as an internal audit and/or advisory to the Divisions of Equans France.

Clients are invited, if necessary, to contact their commercial or operational contact who relays their request to the Cybersecurity Department of the Company.

B. Legal, Regulatory, and Contractual Requirements

As specified in the Company's and Group's IS Security Policies, entities must comply with the laws, regulations, and contractual commitments concerning them. In the context of Equans France's activities, all cybersecurity requirements to be integrated into the contractual compliance framework must take into account the specificities of the applicable regulations related to:

- Third parties (Ministry, Public Sector, Tertiary, Private...)
- Types of activities (Safety, embedded systems, telecommunications management...)
- Places where services are carried out by Equans France's businesses (Public space, ERP, High-rise buildings, regulated spaces, etc.)

The Legal Department and the CYBER CUSTOMER TRUST program combine their skills to contractually manage these points. For other specific scopes, such as contracts for the defense industry where data with "Restricted Distribution" or even "Secret" mentions are handled, or for activities conducted outside French territory, more restrictive measures prevail in this case over those of this document and the Company's security policy documentary corpus.

C. Information Security in Relations with Suppliers

In cases where the Company uses the services of a third party, the modalities for implementing the principles and security rules must be the subject of a specific document: Security Assurance Plan (SAP), or equivalent, co-written and annexed to the contract. The document used differs on depending on the nature of the service provided:

- For third-party maintainers or contractors working on the Company's IS, the SAP (or equivalent) must be provided by the third party, and the Company amends and/or validates it;
- When it comes to SaaS services entrusted to third parties, the SAP based on the Group's model is then used.
- The clauses of this document are proportional and adapted to the activities subcontracted in these agreements (confidentiality, responsibilities, DICT service levels, audits...). If applicable, the contract includes a compliance clause with applicable regulations (e.g., Defense Secret, GDPR, sectoral...).

D. Risk Management

The M-CISO of Equans France defines and maintains the risk management framework of Equans France. Within the CORPORATE IT Information Systems, risk analyses:

- Are integrated into project management;
- Are based on a standardized methodology: EBIOS RM;
- Are validated by the CISO, reviewed during major changes;
- Use BIAs as input;
- Provide risks, with their probability and impact, according to the matrices present in the Group's risk management policy.

Critical or high risks must be treated so that their level becomes acceptable. Thus, a risk treatment plan is constructed and regularly reviewed.

Within the CLIENT IT Information Systems, risk analyses are mandatory for any so-called sensitive business with a significant impact on Equans France. The CYBER CUSTOMER TRUST FRANCE program will ensure for these businesses:

- The assessment of the risk level prior to the submission of the response;
- Monitoring the risk level throughout the life of the business;
- Relies on the EBIOS RM methodology by default;
- Are validated by the RISK COMMITTEE of Equans France and/or by the General Management of the Business Division.
- Use BIAs as input;
- Provide risks, with their probability and impact, according to the matrices present in the Group's risk management policy.

E. Data Classification and Protection

The Company identifies 4 levels of information confidentiality: Public [TLP: WHITE], Internal [TLP: GREEN] default level, Restricted [TLP: AMBER / AMBER-STRICT], Secret [TLP: RED]. These levels are based on business needs in terms of sharing or restricting information. All information assets have an owner and have a classification label.

Data owners:

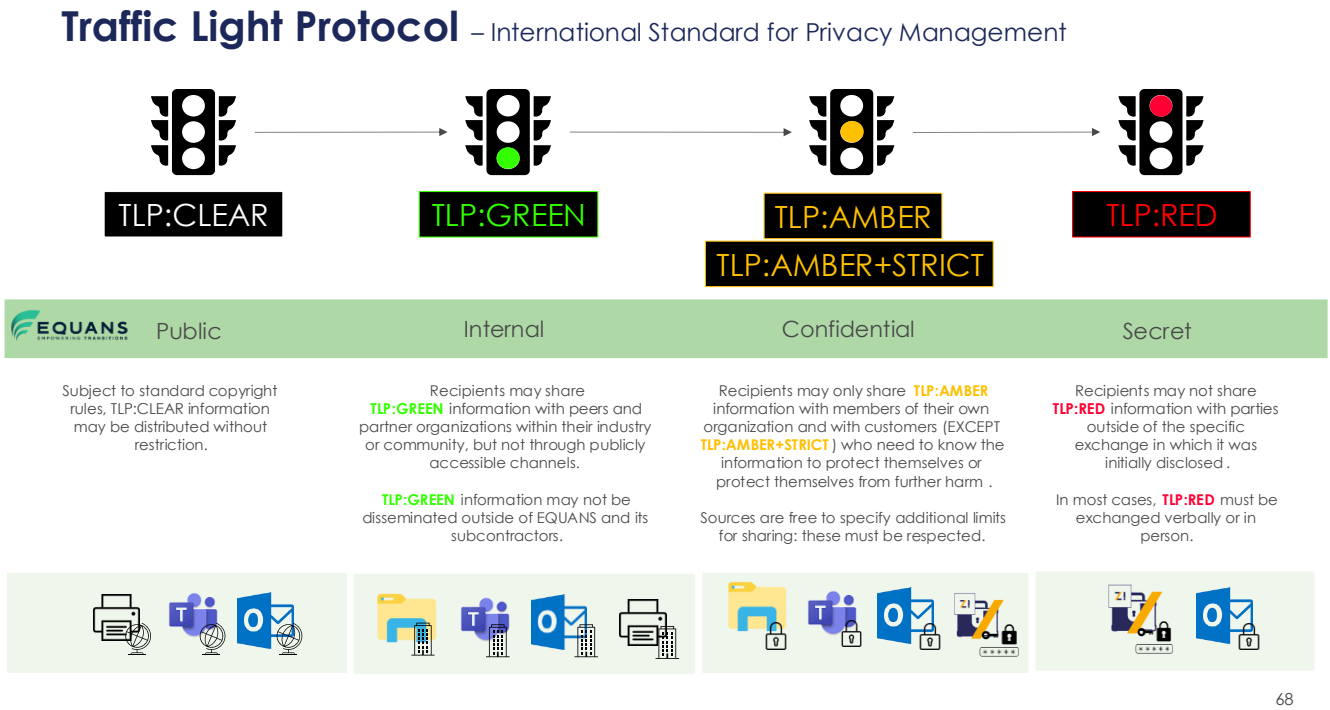
- Set the correct classification level;
- Ensure that operationally, the concerned IS components ensure the appropriate DICT levels;
- Establish adequate authorizations to access information (based on the principles of least privilege and need-to-know);
- Provide requirements in terms of business continuity.

The Company shares confidential information only in the presence of a contractual agreement with a confidentiality clause or with a non-disclosure agreement (NDA). Any User, noticing or suspecting an incident involving data, immediately contacts their supervisor who directly reports the information to the IS Department.

General Data Protection Regulation (GDPR):

The Company's DPO ensures compliance with GDPR. It relies on the register of processing activities (Article 30 of GDPR), kept up to date thanks to the information provided by data owners. In accordance with the recommendations of the CNIL, the Company conducts a Data Protection Impact Assessment (DPIA) when "the processing is likely to result in a high risk to the rights and freedoms of individuals." The Charter for the use of IT resources specifies the obligations of Users regarding the processing of Personal Data.

Information relating to the Protection of National Defense Secrets: The processing of this information is governed by the Security Officers and IS Security Officers of the legal entities of Equans France. The CORPORATE IT IS is not authorized to store information subject to the following regulations (IGI 1300, IM900, II901).



F. Security Measures Applicable to Individuals

As part of hiring, the Company's recruitment teams conduct security checks proportional to business requirements so that the candidate can fully collaborate, for example, in case of a need for "Defense Secret" clearance. All Users of the Company must confirm that they have read the Charter for the use of IT resources, specifying the terms of use of the IS and the resources made available to them (including data confidentiality management). The charter is distributed and accessible to all Users upon their arrival. It is annexed to the internal regulations of the entities specifying the penalties incurred. The Company raises awareness among its Users about IS security (risks, scenarios, best practices...) by providing adapted materials, e-Learning, and during specific events (phishing awareness, cybersecurity training for user groups, intervention during business seminars...).

Teleworking is authorized under the following conditions:

- The employee's tasks allow for teleworking;
- The employee's request has been validated by their management;
- The employee commits to using only the equipment (PC, smartphone, tablet...) provided by the Company for their professional activity.

3. SECURITY PRINCIPLES - CORPORATE IT SECURITY

A. Asset Management

The Company's IT resources are inventoried in a CMDB. A procedure details the attributes collected and recorded in this repository. It includes at least information about the asset owner, its criticality level, and its classification. The CMDB is updated to track changes to assets (e.g., an operating system version upgrade) as well as their retirement. Procedures govern the lifecycle of assets:

- When setting up a new asset, its configuration complies with hardening guidelines, according to the "security by design" principle.
- The processes for Operational Condition Maintenance (OCM) and Security Condition Maintenance (SCM) are detailed in specific procedures, by type of asset.
- Monitoring tools report malfunctions and security events from assets.
- The decommissioning/recycling/removal of an asset is done in accordance with security principles, regulations, and business needs: data retention period, proof of destruction, storage media destruction procedures...

B. Access Control

Every User must be authenticated when accessing the Company's IS, in compliance with the authorizations they have. The Company logs the access of all Users to the IS and the most sensitive actions. Requests for application authorizations follow best practices and, in particular:

- Requests are logged in ticket management tools;
- Access is granted according to the principles of 'least privilege' and 'separation of duties';
- Roles are assigned by job profiles.

The Company regularly conducts authorization reviews, the frequency of which is adapted to the sensitivity of the accesses. Privileged access to the IS by administrators is reinforced: password complexity adapted, specific multi-factor authentication (MFA), administrator charter, secure protocols, physical keys, bastion... Access to the Company's IS from outside (teleworking, third-party application maintenance...) relies on the use of a 'Zero Trust' solution with MFA.

C. Identity Management

Identity management within the Group and its entities is based on the 'Group Identifier' (GID): a unique alphanumeric identifier that allows identifying a User within the Group's identity repository. Anyone accessing the Group's CORPORATE IT IS must have a GID, excluding 'Office 365 guests'. The allocation of a GID must be done through the Group's solution, providing information to uniquely identify the User. Even after leaving the Group, a GID is never reused for a different person. A person retains their GID even if their status changes (e.g., following internalization).

All access to the technical solutions and business applications of the entities must rely on the GID through the Group directory. It is the responsibility of Human Resources and the management line of the Company and its entities to manage the lifecycle of identifiers by:

- Anticipating the arrivals, departures, and mobility of individuals (internal and external);
- Conducting an annual review for externals whose engagement duration exceeds 12 months before renewing rights;
- Reporting the end of a contract/mission as soon as possible and ensuring it is effective in the IS the week following the end date.

The emergency deactivation procedure of an account can be triggered upon request from Human Resources or by the CERT (in case of compromise). This ensures the deletion of all access rights within 24 hours. Personal administration accounts must rely on specific identifiers, distinct from standard personal accounts. The authentication rules for these accounts are reinforced (see next section). Duties and usage are specified in the Administrator Charter. Administrators with high and global privileges (domain administrators, etc.) sign a commitment.

D. Authentification

Users of the Company's CORPORATE IS commit to respecting the directives present in the Charter for the use of IT resources, in particular:

- Keeping authentication information secret;
- Respecting password complexity rules;
- Using different authentication information between professional and personal uses;
- Using a personal administration account for system administration tasks, which differs from the standard usage account.

Passwords are encrypted in transit and in the databases where they are stored. Access to the IS relies on the use of SSO and MFA mechanisms. SSO authentication is based on the Group's identity federation to associate all their accesses with their main account. This practice concerns all applications, including SaaS ones.

E. Information Security in the Use of Cloud Services

The principles stated below are specific to the scope of the IS hosted within Cloud Service Providers (CSP). All principles from other themes must also be respected in the Company's Cloud spaces (e.g., vulnerability management, access control, etc.).

The Company's Cloud spaces are organized in a tree structure whose "root" level is managed by the Group. Within these spaces, the management of accounts, resources, and projects is aligned with the Group's directives (identified owners, regular account reviews, secure authentication, ISP...). The filtering rules at the network level and on the servers are as fine as possible. The Company relies on the Group's IP Address Management (IPAM) tool. Connections to the Group's network core are subject to specific requirements.

The exposure of assets to the Internet relies on security solutions: firewall, WAF (Web Application Firewall), load balancers, anti-DDoS solutions, state-of-the-art encryption protocols...

IT resources hosted by CSPs are supervised by Group tools such as Cloud-Native Application Protection Platforms (CNAPP) and are subject to monitoring indicators.

F. Incident Management

The Company has a logging process to collect and protect any information enabling the detection of a security event or the conduct of an investigation following a confirmed security incident. The retention of the collected information is proportional and in accordance with current regulations. A cyber surveillance process relies on this information to trigger alerts sent to the GSOC (Group Security Operational Center), which is part of the CSIRT.

Contributors & roles :

Fonction	Missions
Users	Signalement des incidents de sécurité (avérés ou suspectés) au département cybersécurité de la DSI
IS'S Cybersecurity Department	Monitoring cybersecurity incidents and crises
Other IS Departments	Incident management
CISO and a member of the Management	Triggering the crisis process
CSIRT/GSOC (SLS Cyber Defense)	Real-time monitoring of alerts on assets (workstations, networks, applications...) and incident response
CERT (SLS Cyber Defense)	Management of the crisis at the Group level

Once the security incident is qualified, emergency measures can be taken to limit the impacts and preserve evidence. In parallel with containment, an investigation is launched to identify the characteristics of the incident. Security incidents that have triggered cyber crisis management are tracked and subject to a corrective action plan followed by the Company's CISO.

G. Business Continuity

Based on business needs in terms of availability, the Company has defined Business Continuity Plans (BCP) to maintain business activities despite the occurrence of incidents making all or part of the IS unavailable. The BCP process is detailed in a document that defines:

- The conditions for triggering the plan (including with third parties);
- The conditions for normal resumption of activities;
- The roles and responsibilities of the plan's actors;
- The necessary documentation;
- The communication methods during the plan;
- The methods for controlling the proper functioning of the plan.

The process is updated as needed to take into account changes in the IS that impact it (e.g., a change of provider for SaaS applications, replacement of network equipment, a change in the infrastructure, etc.). The BCP is regularly tested through business continuity exercises. Among the BCPs, we distinguish:

- Operational Continuity Plans: owned and managed by the Businesses;
- IT Continuity Plans: managed by the DSI

H. Cybersecurity Crisis Management

A cybersecurity incident with particular characteristics (especially impact and/or lack of control) triggers the crisis process, which includes:

- The conditions for entering a crisis;
- The conditions for exiting a crisis;
- The roles and responsibilities of the identified actors at each stage;
- The mobilization of crisis units (technical, operational, decisional);
- The means at the service of crisis management;
- The methods for informing the governance of information security;
- The reporting methods associated with the information security management system.
- The crisis management process is subject to regular exercises.

I. Physical Security Mesures

The Cloud hosting sites of the IS used by the Company are restricted access and subject to strict control (e.g., access by authorized badge...). The sites are ISO 27001 certified and comply with the state-of-the-art market standards for physical security (at least Tier III). Access to a large number of premises or offices of the Company is secured by the use of personalized badges. Every visitor must be accompanied from their entry to their exit from the building by an internal person of the Company.

J. User Equipment

The Charter for the use of IT resources provides the rules for using workstations and mobile equipment. The use of workstations is done through a standard personal account, which does not have administration rights. Only software validated by the DSI can be installed on workstations. Administration actions, such as software installation, are done through a process that requires managerial and/or security team validation. Security software protects and analyzes workstations (behavioral antivirus, "zero trust" type remote access, permanent internet filtering, firewall...). The

Company does not allow the use of BYOD (Bring Your Own Device): the use of personal mobile equipment for professional purposes. It provides certain Users with tablets and/or smartphones. These devices are tracked through a centralized management tool. Any theft or loss of professional IT equipment must be reported to the competent authorities (police, gendarmerie, etc.) and to the IT department to proceed with the deactivation of the equipment and, if possible, the deletion of the data.

K. Vulnerability Management

Continuous monitoring of vulnerabilities is conducted by SLS Cyber Defense with the VMCT (Vulnerability Management and Compliance Team) team within the CERT. It allows identifying security flaws and associated patches applicable to IS components to define and implement adapted and proportional reaction plans. Vulnerability scans are performed at least once a week on the Company's IS. The scans rely on: the inventory of the Company's assets to scan: provided by the CMDB (see section on asset management) and provided to the CERT; the instructions (scan frequency, type of scan, etc.) contained in the Group's scan procedure. The Company prioritizes the treatment of vulnerabilities in coordination with the CERT. When it is not possible to remediate a vulnerability, a risk analysis is conducted (see section on risk management) and mitigation measures are deployed to lower the risk level. The CERT monitors the Company's remediation plan.

L. Backup

For critical assets, the "3-2-1" backup rule is preferred (3 copies, 2 types of media, 1 off-site copy), accompanied by the encryption of backups. Backup needs are defined in coordination with the businesses to define the maximum interruption time (Recovery Time Objective, RTO) and the maximum amount of data that can be lost (Recovery Point Objective, RPO). As part of the Disaster Recovery Plan (DRP), backup and restoration tests are regularly conducted to verify the ability to meet business needs. Backups are deleted when the maximum retention period, set according to business needs, is reached. Regular checks verify the proper application of this principle. Backup systems are monitored, logs and audit trails are kept. The proper execution of backups is verified daily.

M. Network Security

The Company operates a segmented architecture with logical zoning based on usage, including:

A zone grouping servers that host services intended to communicate with the outside;

A private zone grouping servers that are not intended to communicate with the outside.

Devices and filtering rules are implemented to define access to the different zones. Authorized exchanges between these different zones are defined based on risk analysis; they are filtered, monitored, and controlled. Filtering follows the principle that any exchange not explicitly authorized is prohibited. Each request for inter-zone rule changes is subject to a formalized and tracked request and formal validation by the security department. Flows to or from the Internet are filtered and monitored. When an application is exposed to the Internet, it is protected by a WAF (Web Application Firewall) in blocking mode. The use of unsecured, unsupported, or end-of-life protocols is prohibited.

N. Secure Development Lifecycle

Applications developed by the Company's Users must meet the Group's security requirements. The development tools used within the Company are selected by the DSI teams, which ensure the application of updates and security patches. For application development, teams rely on best practices derived from code quality standards and those specific to the Company. Security standards are also respected (e.g., absence of passwords in the code). Projects are documented (Technical Architecture File, architecture diagrams, etc.). Source codes are stored in a centralized repository ('repository') with secured access. Tools check the quality of the code and report security flaws. The lifecycle of external code libraries is monitored by the DSI and cybersecurity teams; if necessary, prior validation by the cybersecurity team may be requested before implementation.

O. Change Management

A change management process is in place within the Group and the Company. All changes are logged in a ticket tool. Changes that have a significant impact on the Company's IS are analyzed during a CAB (Change Advisory Board), whether these changes are initiated at the Company or Group level. The following elements are analyzed:

- The objective/reason for the change;
- The impact analysis;
- The back-out procedure;
- The batching;
- Communication management...

The Company distinguishes several non-production environments (e.g., development, testing, pre-production) to secure production deployments and minimize service downtime.

4. SECURITY PRINCIPES - CLIENT IT SECURITY

As a preamble, the organizational principles defined in the section "2. COMMON PRINCIPLES" apply to CLIENT IT and are supplemented by the following points:

A. Security Principles Applicable to CLIENT IT

The contract and contractual elements prevail over Group policies. The CLIENT defines the expected security level for the services provided by Equans France's businesses. Security requirements must be explicitly transmitted. They can be formalized in the form of:

- Contractual clauses;
- Security Assurance Plan annexed to the contract;
- Other contractual documents (FTM, Service Order...).

Security requirements must be balanced against applicable law. CYBER CUSTOMER TRUST stands alongside Equans France's businesses to precisely analyze the compliance and regulatory framework of the business, taking into account the applicable regulatory requirements:

- For third parties (CLIENT, SUBCONTRACTOR);
- For activities carried out by Equans France's businesses (Operation, Maintenance, Integration...);
- For activity domains (Defense, Security, Safety);
- For places of execution of these activities (Public space, ERP, High-rise buildings...).

CYBER CUSTOMER TRUST can be called upon for each new contract or for any renewal. For any questions: cct.france@equans.com

B. Incident and Crisis Management

The Cybersecurity Department of Equans France provides its support in the field of Cybersecurity to the Business Divisions. In case of high risk, it can call upon the FAST INCIDENT RESPONSE device composed of Equans interns and contractors qualified as PASSI by ANSSI. In case of a major incident, the CLIENT must respect the governance of their business and contact their BUSINESS MANAGER, who will escalate to the teams of the CYBERSECURITY Department of EQUANS France. For any questions: cct.france@equans.com

C. General Data Protection Regulation (GDPR)

For any request related to GDPR or for any exercise of rights, contact: privacy.france@equans.com

5. TERMINOLOGY

- **BIA - Business Impact Analysis**: Process that allows identifying and evaluating the potential impacts of a business interruption on a company.
- **CCT - Cyber Customer Trust**: Equans Group program aimed at reducing the exposure to so-called "cybersecurity" risks of activities carried out for its clients, integrating a Digital component.
- **CERT - Computer Emergency Response Team:** For the Group, this function is provided by SLS Cyber Defense. The CERT has the following missions: sharing knowledge (security monitoring, awareness, and training), vulnerability assessment, and crisis management.
- **CMDB - Configuration Management DataBase:** Configuration management database: repository that serves as a data warehouse for IT installations. It contains data relating to a set of IT assets, as well as descriptive relationships between these assets.
- **CNIL - Commission Nationale de l'Informatique et des Libertés**: In France, the CNIL is the regulator of personal data. It supports professionals in their compliance efforts and helps individuals control their personal data and exercise their rights.
- **CSIRT - Computer Security Incident Response Team:** For the Group, this function is provided by SLS Cyber Defense. The CSIRT has the following missions: detection of cybersecurity events, triage and analysis of these events, investigation and incident response, cyber threat management.
- **DICT - Availability, Integrity, Confidentiality, Traceability:** (In English, CIAT: Confidentiality, Integrity, Availability, Traceability) characteristics that the owner or manager of the information wants to see realized to ensure that security is met for their data.
- **DPO - Data Protection Officer:** Person in charge of the protection of personal data processed by an organization (administration, company...).
- **ISP - Integration of Security in Projects**: One of the fundamental elements of the "security by design" approach. It allows anticipating security needs and protecting companies against the main risks they may face in their digital activities. Often associated with frameworks or methodologies based on the IT risk approach, ISP supports projects from start to finish.
- **MFA - Multi-Factor Authentication:** Method that grants access only if the user presents two or more authentication factors from these types of factors: something you know (a password, a PIN code), something you have (a "hard token", a smartphone with a "soft token" application...), something you are (biometrics such as a fingerprint, facial recognition...).
- **NDA - Non-Disclosure Agreement:** An agreement between two entities that obliges one of these entities to keep certain information confidential that the other will communicate to them. The agreement can also be "mutual," meaning that both entities agree not to disclose certain exchanged information.
- **GDPR - General Data Protection Regulation**: EU regulation that constitutes the reference text regarding the protection of Personal Data.
- **CISO - Chief Information Security Officer:** Defines and develops the information security policy of their company. They are responsible for its implementation and ensure its monitoring. They provide advice, assistance, information, training, and alerts.
- **SaaS - Software as a Service:** "Software as a Service": a software distribution model. It allows a third-party provider to host applications and make them available to customers via the internet.

- **IS - Information System:** Set of processes, organizational resources, hardware, and software of the Company allowing the acquisition, generation, processing, storage, destruction, dissemination, transmission, or access to electronic information within the Company.
- **SSO - Single Sign-On:** Method allowing a user to access multiple computer applications (or secure websites) by performing only one authentication.
- **VPN - Virtual Private Network:** A system that creates a direct link between remote computers, isolating their exchanges from other traffic on public telecommunication networks.