Security Insurance Plan

ISS Team

Status : Approved

Version 1.5

CYBERSECURITY!
everyone's BUSINESS

BUREAU VERITAS 1828

BUREAU VERITAS

Move Forward with Confidence

Public	Internal	Restricted	Secret
X			

Approvers

Name	Position	Date
Julien ANICOTTE	GCISO	28/07/2018
Legal, Risk & Compliance Department		18/09/2018

Versions

Version	Author	Nature of the modifications	Date
1.0	Meryem OUKEMENI	Validation & Diffusion	27/07/2018
1.3	Meryem OUKEMENI	Contractual Security	26/09/2018
1.4	Meryem OUKEMENI	Title modification	17/10/2018
1.5	Youness TASTIFT	Adaptation for third parties only	17/01/2019

Reference documents

Document title	Document Name
Global IS/IT Charter	Global IS-IT Charter v1.0
Physical Security Policy	Physical Security Policy
Logical Access Policy	Logical Access Policy
Development and Maintenance of Applications Policy	Development and Maintenance of Applications Policy
Classification of IT Resources Policy	Classification of IT Resources Policy
Network Security Policy	Network Security Policy

Classification

Level	Confidentiality
C1	Public

Glossary

AWS means Amazon Web Services.

CIAT refers to the fundamental principles of: security Confidentiality, Integrity, Availability, and Traceability.

CISO means Chief Information Security Officer.

GDPR means General Data Protection Regulation. The regulation aims to ensure data protection and privacy for all individuals within the European Union and the European Economic Area

IaaS means Infrastructure as a Service. A form of cloud computing that provides virtualized computing resources over the internet.

Information System means integrated set of components (including IT equipment) for collecting, storing, and processing data and for providing information.

ISS means Information System Security.

ISS Policies mean Information System Security Policies which include the Global ISSP and the Operational Policies. Set of documents defining the framework of Information System Security (ISS) through governance principles and pragmatic rules, which shall be implemented across the Bureau Veritas Group.

IT assets

LDAP means Lightweight Directory Access Protocol.

Malware means (short for malicious software) any software used to disrupt computer or mobile operations, gather critical information, gain access to private Information System, or display unwanted advertising. The term refers to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

NDA means Non-Disclosure Agreement.

PaaS means Platform as a Service. A form of cloud computing that provides virtualized computing resources over the internet.

Personal Data means any information relating to an identified or identifiable living person ('data subject'); an identifiable living person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

SaaS means Software as a Service. A form of cloud computing that provides virtualized computing resources over the internet.

SFTP means Secure File Transfer Protocol.

SIP means Security Insurance Plan.

TLS means Transport Layer Security. It is a cryptographic protocol that secures end-to-end communications over networks.

SIP summary

The following table summarizes the security commitments that third parties must apply when working with Bureau Veritas. Project owner should read carefully the present document and select the applicable commitments.

A justification must be provided, in the appropriate column of the table, for each commitment that would be selected as “not applicable” or that would not be accepted by third party.

Upon receiving this filled in document, Bureau Veritas will review it and reserve the right to ask for proofs regarding the applicability/compliance with the expressed security requirements.

Paragraph	Security Commitment	Applicable	Accepted	Justification
2.1	Third party must provide Bureau Veritas with necessary information/documents throughout the Security By Design process.	☐ Yes ☐ No	Mandatory	
3.1	Third party must respect Bureau Veritas data classification standard, and if applicable, incorporate it into the application/service.	☐ Yes ☐ No	Mandatory	
3.2	Third party employees/machines having access to Bureau Veritas Information System must be individually identified.	☐ Yes ☐ No	Mandatory	
3.2	Third party must provide Bureau Veritas managers with the necessary security information and answer their security questions.	☐ Yes ☐ No	Mandatory	
3.3	Physical access controls in sites hosting Bureau Veritas data must be compliant with Bureau Veritas “Physical Security Policy".	☐ Yes ☐ No	Mandatory	
3.3	Hosting premises must be protected with an Intrusion Detection System (alarms and video surveillance).	☐ Yes ☐ No	Mandatory	
3.3	Access to the server rooms must use a multi-factor authentication and must be performed via an individual code entry.	☐ Yes ☐ No	☐ Yes ☐ No	
3.3	Third party must agree to apply additional security measures, recommended by ISS team based on the risk assessment, to control and protect physical access.	☐ Yes ☐ No	☐ Yes ☐ No	
3.3	All the gates giving access to sensitive areas must be locked and the access must be granted only to eligible users.	☐ Yes ☐ No	Mandatory	
3.4.1	Third party must apply security measures and controls stated in 3.4.1 to secure its network.	☐ Yes ☐ No	Mandatory	
3.4.2	Backup and retention policies must be defined with the application owner.	☐ Yes ☐ No	☐ Yes ☐ No	
3.4.2	Backup and retention policies must take into account the classification of the data according to the CIAT criteria.	☐ Yes ☐ No	Mandatory	

3.4.2	All the Backups must be replicated on a secondary site.	☐ Yes ☐ No	Mandatory
3.4.2	All the data must be stored, backed-up and purged in accordance with the laws and regulations applicable to personal data protection and the contractual obligations.	☐ Yes ☐ No	Mandatory
3.4.3	The encryption must be performed when needed depending on the classification of the data according to the CIAT criteria, the device's type and capability.	☐ Yes ☐ No	Mandatory
3.4.3	Data must be encrypted in transit on external public networks, including the internet.	☐ Yes ☐ No	Mandatory
3.4.3	All the data must be encrypted in the databases. All the data exchange must be performed using secure protocols.	☐ Yes ☐ No	Mandatory
3.4.3	The exchange of confidential files between internal users and the third party must be secure, using a method recommended by ISS team.	☐ Yes ☐ No	☐ Yes ☐ No
3.4.3	Any devices were Bureau Veritas confidential data resides must be encrypted.	☐ Yes ☐ No	Mandatory
3.4.4	Third parties must provide Bureau Veritas with necessary access/information/approval to conduct the vulnerability scans/ penetration testing when necessary.	☐ Yes ☐ No	Mandatory
3.4.4	Third party must deploy corrective actions as recommended by ISS team before the application go live.	☐ Yes ☐ No	☐ Yes ☐ No
3.5	Every new application authentication process must be performed via the LDAP.	☐ Yes ☐ No	☐ Yes ☐ No
3.5	The strength of passwords for all applications must be compliant with Bureau Veritas "Logical Access Policy", as described in 3.5.	☐ Yes ☐ No	Mandatory
3.6	Every new web application developed must comply with the security policy "Development and Maintenance of Applications Policy" and comply with the "Best practices and security requirements for web development" document based on the OWASP development guide.	☐ Yes ☐ No	☐ Yes ☐ No
3.7	Third party must define a formalized process to manage information security incidents.	☐ Yes ☐ No	☐ Yes ☐ No
3.7	Third party must define a standard canal of communication to report to Bureau Veritas all the security incidents or breaches that may threaten the security of its information system.	☐ Yes ☐ No	☐ Yes ☐ No
3.7	When the incident concerns applications or assets owned by Bureau Veritas, it is mandatory to use BV standard tools for the reporting.	☐ Yes ☐ No	☐ Yes ☐ No
3.8	Third party must comply with The GDPR compliance framework for Bureau Veritas.	☐ Yes ☐ No	☐ Yes ☐ No
3.8	Third party must communicate their GDPR roadmap, timeline and compliance plan.	☐ Yes ☐ No	☐ Yes ☐ No
3.9	The contract to be concluded between Bureau Veritas and the third party must include the more detailed security requirements mentioned in 3.8.2	☐ Yes ☐ No	Mandatory

SUMMARY

1. GENERALITIES

1.1. PURPOSE OF THE DOCUMENT

The purpose of this document is to ensure that the services provided to Bureau Veritas by third parties respect the security level defined by Bureau Veritas, and thus, ensure that Bureau Veritas security systems remain effective, robust and resilient.

This document gives guidelines regarding the information security insurance mechanisms and describes the set of measures and rules that should be applied by Bureau Veritas's partners, service providers and subcontractors in order to protect the information systems of Bureau Veritas.

1.2. OBJECTIVES OF THE DOCUMENT

The objectives of the Information Security Insurance Plan are to:

- Take all the necessary steps to ensure that all important corporate assets are at all times protected, available and accurate to support Bureau Veritas operations;
- Define guidelines for securing the services provided by Bureau Veritas service providers, subcontractors and partners, that need to access or manipulate Bureau Veritas' Information System;
- Ensure that Bureau Veritas security systems are effective, robust and resilient;
- Set up contractual security requirements to be included in contracts with service providers, partners and subcontractors;
- Apply the security measures as recommended by Bureau Veritas in order to protect its technical architecture;
- List the different actions to ensure the compliance with Bureau Veritas Security Policies;
- Present applicable security measures and insurance precautions according to business needs.

1.3. DOCUMENT AUDIENCE

- This document is addressed to Bureau Veritas's partners, service providers and subcontractors

2. SECURITY GOVERNANCE

2.1. SECURITY BY DESIGN

Security by Design is an approach to security that allows formalizing infrastructure design and automating security controls in order to build security into every part of the project development life cycle. The aim is to ensure that security is taken into account since the beginning of any project and all along its life cycle, and understood, accepted and validated by all the stakeholders (project owner, project manager, developers, CISO, third-parties, etc.).

The project life cycle approach, adopted by Bureau Veritas for all the development projects, is divided into five phases:

- Pre-Study
- Initiation
- Design
- Execution
- Closure

Each phase involves one or several gates, requiring specific deliverables to be validated.

The different gates of the project life cycle are as follow:

- **Pre-study Go/No Go:** Authorize the start of a pre-study to collect information required to define project frame;
- **Project Go/No Go:** Confirm we're doing the right project or Stop;
- **Project Kick Off:** Confirm project team is ready & fully operational;
- **Design review:** Confirm design is OK and we're ready for the solution build;
- **Go Live:** Confirm the solution is ready to be used by the end users;
- **Project Closure:** Confirm the project activities can be closed and handover to the project team and the application owner.

The security team must take part in the project life cycle. In every gate, the ISS team will ask for deliverables in order to verify that all the security requirements are respected. After analyzing the deliverables results, the Security Team will give a Go/No Go decision, if the Project Owner decides to proceed despite a No Go from the CISO, the ISS Team will disengage itself and the developed project might not be supported by BV teams and infrastructure.

Bureau Veritas's partners, service providers and subcontractors must provide the project owner and ISS team with the necessary information/ security documents (Such as: Security policies, architecture diagrams, vulnerability scans, audit reports, business continuity plan, incidents management procedure) needed to verify the security requirements.

If the Analyzes results in a remediation plan / action plan, Bureau Veritas's partners, service providers and subcontractors must agree to deploy it and provide Bureau Veritas with the necessary proofs that the plan was successfully implemented.

3. PROTECTIVE MEASURES

3.1. DATA CLASSIFICATION

The data classification process aims at qualifying the importance of the data manipulated by Bureau Veritas and its business partners (service providers, suppliers, subcontractors) according to the predefined security criteria and levels.

The protection of data applies to all aspects of the information, guaranteeing an appropriate protection level whatever its form.

The “Classification of IT Resources Policy”, lists all the criteria and levels that must be applied to Bureau Veritas’s IT assets.

Every document produced in (or produced for) Bureau Veritas must be labelled and marked with the corresponding confidentiality level by its owner.

The classification criteria adopted for the classification of Bureau Veritas’s data are:

- **Availability (A)**: ability of the information system to ensure the performance of the processing operations and access to the information under previously defined condition;
- **Integrity (I)**: ability of the information system to ensure to limit risks of unintentional or intentional alteration;
- **Confidentiality (C)**: ability of the information system to restrain access to authorized people that need to know and need to use information;
- **Traceability (T)**: ability of the information system to provide access and changes traces and potentially other kind of information.

Classification levels of confidentiality:

CLASSIFICATION		DEFINITION
C1	Public	Information created in order to be published **publicly**. Unauthorized disclosure to the public of public information will not prejudice Bureau Veritas, or his partners, suppliers or clients.
C2	Internal	Information that can be accessed by **all employees or a large majority of them**. It is not meant to be published publicly. Unauthorized disclosure to the public of internal information should not prejudice Bureau Veritas or, his partners, suppliers or clients.
C3	Restricted	Information for a **specific audience**. Unauthorized disclosure to the public of restricted information can cause a significant financial prejudice, can result in legal consequences or may damage the reputation of Bureau Veritas, or his partners, suppliers or clients. This applies in particular to information that can be precious for competitors, or can put in danger the security of Bureau Veritas.
C4	Secret	Strictly limited access information, for **specific employees** identified by their names within Bureau Veritas. Unauthorized disclosure to the public of secret information can cause a significant prejudice to Bureau Veritas, affect his objectives on the long term, can result in serious legal consequences, cause a significant financial prejudice or may seriously damage the reputation of the company, or of his partners, suppliers or clients.

Classification levels of integrity:

CLASSIFICATION		DEFINITION
I1	None	The integrity of the asset may **not be controlled.** The unauthorized modification or destruction of information or information assets can only have an extremely limited impact on Bureau Veritas, or on his partners, suppliers or clients.
I2	Detectable	The information may not be complete, provided **the alteration is identified.** If not corrected, the modification is acceptable. The unauthorized modification or destruction of information or information assets can only have a limited impact on Bureau Veritas, or on his partners, suppliers or clients.
I3	Controlled	The asset may not be complete, provided **the alteration is identified and integrity can be restored.** The unauthorized modification or destruction of information or information assets can have a significant impact on Bureau Veritas, or on his partners, suppliers or clients.
I4	Intact	The asset must **be intact** (not modifiable). The asset must have the mechanism making impossible to alter data. The unauthorized modification or destruction of information or information assets can have a very unfavorable impact on Bureau Veritas, or on his partners, suppliers or clients.

Classification levels of Availability:

CLASSIFICATION		DEFINITION
A1	None	Permanent loss or unavailability acceptable for **more than 48h.** The asset loss or access interruption to an asset can only have an extremely limited impact on Bureau Veritas, or on his partners, suppliers or clients.
A2	Standard	Unavailability or temporary loss acceptable **between 12-48h.** The asset loss or access interruption to an asset can only have a limited impact on Bureau Veritas, or on his partners, suppliers or clients.
A3	High	Unavailability or temporary loss acceptable **between 4-12h.** The asset loss or access interruption to an asset can have a significant impact on Bureau Veritas, or on his partners, suppliers or clients.
A4	Critical	Unavailability or temporary loss acceptable **less than 4h.** The asset loss or access interruption to an asset can have a very unfavorable impact on Bureau Veritas, or on his partners, suppliers or clients.

Classification levels of Traceability:

CLASSIFICATION		DEFINITION
T1	None	The asset requires **no traceability.** The lack of traces or proofs of executed actions on the asset will not cause any prejudice to Bureau Veritas, or to his partners, suppliers or clients.
T2	Standard	The asset requires traceability corresponding only to **Who** and **When.** The lack of traces or proofs of executed actions on the asset can cause a limited prejudice to Bureau Veritas, or to his partners, suppliers or clients.
T3	High	The asset requires traceability corresponding : **Who ? When ? From Where ? What? Where?** But also, it will provide a **general description the transaction**. The lack of traces or proofs of executed actions on the asset can cause a significant prejudice to Bureau Veritas, or to his partners, suppliers or clients.
T4	Imputative	The asset requires a full monitoring: **Who? When? From where? What? Where?** A **full description of the transaction** (general and detailed description) and it will require a **retention requirement of internal objectives**. The lack of traces or proofs of executed actions on the asset can cause a very severe prejudice to Bureau Veritas, or to his partners, suppliers or clients.

The classification of the data is done collaboratively by the project owner and stakeholders from the business. Once the classification according to one of the security criteria stated before is of level 3 or 4, a Risk Assessment should be conducted and a non-exhaustive list of security measures and additional recommendations may be applied depending on the security criteria and levels:

	Confidentiality	Integrity	Availability	Traceability
Level 1			- Storage on user machine only - Storage on devices managed by the user	- Implement basic technical monitoring
Level 2	- Implement access with individual account (login + password) - Rights management based on the need-to-know - Semiannual review of access rights - Semiannual review of access logs - Prefer corporate solutions to exchange the data	- Log access to the data - Grant write rights based on the need-to-use - Regular review of access and write rights	**Application** - Standard backups in datacenters - Back-up data daily / on alternate days - Check backups at least once a year **Workstation** - Synchronize data when connected to the corporate network	- Log at least who and when
Level 3	- Implement Strong authentication - Encrypt data in transit - Encrypt workstation HDD / Shares - Mandatory use corporate solutions to exchange data - Lock up data on physical supports (paper documents, external HDD ...) when not in use - Mandatory print in a confidential way - Monthly review of access rights - Monthly review of access logs	- Implement versioning of document - Backup of the data at each modification - Available rollback on changes - Implement 4 eyes review process	**Application** - Back-up data every day - Check backups every month **Workstation** - Workstation synchronized with DC	- Log at least who, when, from where, what, where - Provide a general description or the transaction
Level 4	- Weekly review of access rights - Weekly review of access logs - Maintain the list of authorized access up-to-date (monthly ?) - Never store data on removable media (USB key, external HDD ...) - Print on a dedicated printer network - Mandatory storage on premise - Forbid exchange outside BV Group - Store paper documents and removable media in a vault	- Block modification functionnalities on data - Use non-editable format (e.g. PDF) - Archive the data (read-only access)	**Application** - Back-up data according to SLA: in less than 4h (even continuous backup) - Check backups every months - Include the process/application/asset in the Business Continuity Plan (Including Disaster Recovery Plan) **Workstation** - Instant replication of data on the (corporate ? external ?) network (no warranty)	- Log at least who, when, from where, what, where - Provide a full description of the transaction (general and detailed description)

3.2. HUMAN RESOURCES SECURITY

3.2.1. EXTERNAL PARTNERS/SERVICE PROVIDERS AND SUBCONTRACTORS REQUIREMENTS

Every partner, service provider and subcontractor having access to Bureau Veritas's Information System must be individually identified.

Similar to Bureau Veritas employees, the external employees are subject to penalties if they do not respect the IT Charter and the Internal Regulations of Bureau Veritas. They will be handed these two documents and must sign a declaration ensuring he have taken note of these documents and of applicable penalties if they are not respected. They are also obligated to respect the physical security rules applied within Bureau Veritas.

External employees having access to Bureau Veritas's information system must be qualified and trained to respect cyber hygiene practices; in order to keep Bureau Veritas' data safe and protected.

3.2.2. INFORMATION TO PROVIDE BY EXTERNAL PARTNERS/SERVICE PROVIDERS AND SUBCONTRACTORS

Bureau Veritas's partners, service providers and subcontractors must provide Bureau Veritas managers with necessary security information and answer their security questions.

The required security information and documents serve as a guarantee that the third party implements security measures in order to ensure the safety of Bureau Veritas.

The security documents only includes those relevant to the scope of the service provided and that justify how it will be carried out in a secure manner (security roadmap, security policies, internal and formalized security procedures that are applied…)

3.3. PHYSICAL SECURITY

3.3.1. HOSTING SITES SECURITY

The physical access control in external sites hosting Bureau Veritas's data must be compliant with Bureau Veritas "Physical Security Policy". The policy can be communicated to Bureau Veritas's service providers, partners and subcontractors under an NDA.

The premises must be protected with an Intrusion Detection System (alarms and video surveillance). The duration and modalities of the recordings retention must be in accordance with legal and regulatory constraints.

The access to the server rooms must use a multi-factor authentication and must be performed via an individual code entry.

Based on the site's risk assessment performed by Bureau Veritas ISS team, the third party is responsible of applying the appropriate security measures; i.e. video surveillance, alarms and a security team in place.

3.3.2. PHYSICAL ACCESS CONTROL

All the supplier's premises must be equipped with a reception area, located in a public area, in charge of the verification of the visitors' identity, registering the entries and exits of visitors, providing the security requirements of the site:

- **For supplier's employees**: the access to the premises must be performed via individual badges that are specific to the premises location.
- **For supplier's visitors**: After communicating their identity information, the visitors must be accompanied by an employee during their visit.

In the event of usage of information system that hosts or manipulate Bureau Veritas's data on supplier's site, refer to paragraph 3.3.1.

All the gates giving access to sensitive areas must be locked and the access must be granted only to eligible users.

3.4. OPERATIONS AND COMMUNICATIONS MANAGEMENT

3.4.1. NETWORK SECURITY

The "Network Security Policy" is published and is available to Bureau Veritas's partners, service providers and subcontractors under an NDA.

The following security measures and controls must be applied by the supplier on its network infrastructure:

- Boundary must be protected with a firewall with ingress and egress filtering;
- Public facing servers must be in a defined De-Militarized Zone (DMZ);
- Host Intrusion Detection and Prevention must be implemented on hosts and be actively monitored;
- Hardening must be implemented;
- All the servers must be protected using regularly updated anti-virus software or using other appropriate countermeasures against viruses and malwares;
- Operating Systems must be maintained and updated as well as the applications installed on them;

- The network and hosts must be regularly scanned for unauthorized or vulnerable configurations (Vulnerability scanning);
- Internal network segmentation must be implemented.

In order to protect Bureau Veritas's network from external threats when connected to third parties networks, in addition to the set of security measures mentioned above the following measures must be applied:

- Bureau Veritas and third parties environments must be separated;
- Only the required flows may be authorized (IP source & destination filtering and port destination filtering).

3.4.2. BACKUPS AND DATA RETENTION MANAGEMENT

A backup procedure must be formalized and regularly tested. All the servers must be backed up and retention or backup policies must be defined with the application owner.

The backup and retention policies must take into account the classification of the data according to the CIAT criteria (as set in the paragraph 3.1).

All the Backups must be replicated on a secondary site.

All the data must be stored, backed-up and purged in accordance with the laws and regulations applicable to personal data protection and the contractual obligations.

3.4.3. DATA ENCRYPTION

The encryption must be performed when needed, depending on the classification of the data according to the CIAT criteria, and on the device's type and capability. Data must be encrypted in transit on external public networks, including the internet.

All the data must be encrypted in the databases. All the data exchanges must be performed using secure protocols (SFTP, TLS) with non-vulnerable cipher protocols.

The exchange of files between internal users and external parties (partners, service providers, subcontractors) must be secure, using a method recommended by ISS team.

The hard drive encryption must be deployed on computers containing Bureau Veritas's information, in order to protect it by converting it into unreadable code that cannot be deciphered by unauthorized people. Basic disk encryption must be used to prevent unauthorized access to data storage.

3.4.4. VULNERABILITY SCANS AND PENETRATION TESTS

There are two options of Security Assessments for web applications in Bureau Veritas:

- **Vulnerability Scans**

Vulnerability Scans allow detecting and classifying application weaknesses and configuration errors (default accounts and passwords, exposure of sensitive data, security errors).
Vulnerability Scans are performed directly by Bureau Veritas ISS Team using a dynamic application security testing tool.
The scanner generates an automatic raw data report with detailed information about found vulnerabilities and remediation plan.
ISS Team will analyze this data and write a condensed report with guidelines on corrective actions to be taken before the application go live.
The Vulnerability Scan is performed when an application owner has submitted a request to ISS Services or when a security risk was identified.

- **Penetration Testing**
  Penetration tests are more thorough security tests than Vulnerability Scans as they are operated by a human.
  The Pentester will simulate a hacker attack in order to penetrate a website.
  Such tests are closer to real situations as they are a simulation of real attacks conducted by hackers.

Third parties must provide Bureau Veritas with necessary access/information/approval to conduct security assessments using the two methods mentioned above.

3.5. LOGICAL ACCESS CONTROL

Every new application (SAAS, PAAS, IAAS or on premise) authentication process must be performed via the LDAP.

The “Logical Access Control Policy” is published. The password policy is defined as follow:

The strength of passwords of every user must match the following criteria:

- Minimal length: 8 characters;
- Validity period: 90 days;
- Complexity: the password must have a minimum of 3 elements out of the following:
  - Digital characters;
  - Special characters;
  - Lowercase alphabetical characters;
  - Capital alphabetical characters;
- History: different from the previous 5 passwords used by a user.

The strength of passwords of every administrator must match the following criteria:

- Minimal length: 16 characters;

- Validity period: 90 days;
- Complexity: the password must have a minimum of 3 elements out of the following:
  - Digital characters;
  - Special characters;
  - Lowercase alphabetical characters;
  - Capital alphabetical characters;
- History: different from the previous 10 passwords used by an administrator.

The “Logical access Control Policy” must be respected for all the applications.

3.6. SECURITY DEVELOPMENT

Every new developed web application must comply with the security policy “Development and Maintenance of Applications Policy” and comply with the “Best practices and security requirements for web development” document based on the OWASP development guide.

Bureau Veritas partners and providers must refer to and comply with these documents. Security must be addressed in all the steps of the project life cycle (Refer to paragraph 2.1).

3.7. INFORMATION SECURITY INCIDENTS MANAGEMENT AND RESPONSE

3.7.1. INFORMATION SECURITY INCIDENT PROCESS

Bureau Veritas partners, service providers and subcontractors must define and communicate to Bureau Veritas a formalized process to manage information security incidents. They must additionally inform Bureau Veritas of any security breaches or incidents that may affect Bureau Veritas information system security.

3.7.2. INFORMATION SECURITY INCIDENTS REPORTING

Bureau Veritas partners, service providers and subcontractors must define a standard canal of communication to report to Bureau Veritas all the security incidents or breaches that may threaten the security of its information system.

For security incidents related to applications or assets owned by Bureau Veritas, it is mandatory to use a tool recommended by Bureau Veritas as the main canal of communication.

3.8. PERSONAL DATA PROCESSING

3.8.1. GDPR

The GDPR compliance framework for Bureau Veritas must be respected for all projects that would be developed within Bureau Veritas. Bureau Veritas partners, service providers and subcontractors must comply with this framework.

Bureau Veritas partners, service providers and subcontractors must communicate their GDPR roadmap, timeline and compliance plan.

3.8.2. CONTRACTUAL SECURITY REQUIREMENTS

Every contract to be concluded between Bureau Veritas and a partner, a service provider or a subcontractor must include the following security information:

1- **Hosting:** if the contract is concluded with a cloud service provider for a web application, the service provider should describe all the resources that would be made available for Bureau Veritas. It should also define the geographical location of its datacenters or its cloud service provider (i.e.: AWS) where the data would be stored.

2- **Application security and authentication:** all the security measures and mechanisms applied to secure the application shall be described.
The authentication process must use the LDAP and the password policy must comply with Bureau Veritas Logical Access Control Policy.

3- **Staff management:**
   - **Security training & awareness:** The personnel who would intervene on Bureau Veritas premises or manipulate data must be trained to comply with the security requirements and best practices. The partner, a service provider or a subcontractor must communicate elements of proof showing that their company maintains awareness campaigns.
   - **Access Rights and equipment management:** The partner, a service provider or a subcontractor must manage all the access rights in respect with the “Bureau Veritas Logical Access Control Policy”.
     All the equipment that would be used during the service must be handled in compliance with the “Bureau Veritas User Equipment Policy”.

4- **Reversibility Plan:** when the contract expires or is terminated for any reason whatsoever, the partner, a service provider or a subcontractor shall provide the reversibility services as it will be described in the reversibility plan attached to the contract.

5- **Termination terms:** all the terms related to service termination, data reversibility process at the end of the service under a standard format, restitution of the final copy of the database, final data destruction upon Bureau Veritas consent, shall be defined.

6- **Data at rest, retention policies, backup and data purging**: the partner, service provider or subcontractor shall provide a periodic Data backup service. They shall

at least ensure full recovery of Bureau Veritas Data from D-1, and shall be stored for the entire term of the contract and until completion of the reversibility plan. Bureau Veritas may request that a backup copy be provided at any time, as well as a back-up recovery in case of any event, which may have caused the alteration, total or partial loss of Data. The security measures implemented by the partner, service provider or subcontractor shall be attached to the Agreement.

7- **Data classification:** the data should be classified according to “Bureau Veritas Data Classification Policy” depending on the security criteria and levels.
8- **Architecture:** The security architecture of every application should comply with Bureau Veritas security policies and best practices.
9- **Audit and penetration tests:** describe the frequency of audits, if the audit reports would be communicated to Bureau Veritas, If Bureau Veritas can audit the partner, service provider or subcontractor provider system.
10- **Encryption:** describe the flows encryption mechanisms.
11- **Physical security:** describe the physical security measures made available by the service provider in order to protect Bureau Veritas data.
12- **Data protection** describe the partner, service provider or subcontractor plan, timeline and compliance with GDPR and the measures in place to protect Bureau Veritas personal data.
13- **Disaster Recovery and Business Plan:** describe the security measures that would be applied in case of a disaster.

14- **Security incident management:** Bureau Veritas must be notified of any security breaches or incidents that may affect its information system: this includes business and personal data;
The service provider/partner/subcontractor must describe the security incident escalation process and define the canal of communication that would be used for the security incident tracking and reporting.

15- **Security insurance plan:** The service provider/partner/subcontractor shall comply with the principles and security requirements set out in the Insurance Security Plan annexed to this contract.

3.9. SECURITY POLICIES REFERENCES

PAS Chapter	Security Policy	Security Policy Chapter reference
Data Classification	Classification of IT Resources (Version 1.2)	CITR.1,2,3,4,5,6,7,8,9,10,11
External Partners/Service Providers/ Subcontractors	Supplier Relationship Policy (Version 1.1)	SR.3,4,5,6
Hosting sites security	Physical Security Policy (Version 1.1)	PS.7,9,25,28,31
Physical access control	Physical Security Policy (Version 1.1)	PS.42,43,44,45,46,47,48,49,50
Network security	Network Security Policy (Version 1.1)	NS.11,12,13,14,15,16,22,23,24,25,26 ,27,28,29
Backups and data retention management	Activity Continuity Management (Version 1.0)	AC.11
Data encryption	User's Equipment Policy (Version 1.0) Network Security Policy (Version 1.1)	UE.19 NS.29,39,59
Vulnerability scans and Pentests	Development and Maintenance of Applications Policy (Version 1.1)	DMA.24,25,26
Logical Access Control	Logical Access Control Policy (Version 1.4)	LAC.18
Security development	Development and Maintenance of Applications Policy (Version 1.1)	DMA.12,13,14,15,16,17,18,19
Information security incidents reporting	Management of Security Incidents Policy (Version 1.0)	MSI.25,26,27,28