SECURITY INSURANCE PLAN

STATUS : VALIDATED

VERSION : 2.0

PUBLIC	INTERNE	RESTREINT	SECRET
X			

SUMMARY

GENERALITIES

PRESENTATION OF THE SECURITY INSURANCE PLAN

This Security Insurance Plan (“SIP”) shall apply to any third party (“Third Party”) accessing to Bureau Veritas’ Information System or Data (e.g. when providing Bureau Veritas with a service or when developing a digital partnership).

The objective is to guarantee that third parties comply with Bureau Veritas’ security needs and are aligned with security’s best practices when accessing to Bureau Veritas’ Information System or Data.

This ensures that Bureau Veritas Data is properly safeguarded and its systems remain effective, robust and resilient.

This SIP shall enlist required security measures and controls to be applied and maintained in the scope of the service offered to or partnership developed with Bureau Veritas.

The Third Party is kindly asked to duly fill in the present document and provide appropriate comments and details to help Bureau Veritas assess their security stance. In case of non-compliance with a requirement, it is in the best interest of the Third Party to set forth alternative measures, if any, they deploy to reduce the risk.

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

A filled-in SIP with entries from a Bureau Veritas Third Party becomes a **restricted document (C3)**. Once filled in, the classification level on the footer of the document shall be updated accordingly.

SCOPE AND DURATION

In respect to Bureau Veritas Partners Code of Conduct, the SIP forms an integral part of the contractual relationship between **Bureau Veritas** and:

Company Name	
Company Address	
Point Of Contact details	

The SIP outlines the technical and organisational security measures, implemented by the Third Party, to safeguard themselves and Bureau Veritas Data against unlawful processing, loss, theft, accidental or fraudulent deletion, alteration or destruction, or damage, or unauthorized use or disclosure.

These security measures are applicable to the following scope of service provided to / partnership developed with Bureau Veritas:

They shall remain effective for the complete duration of the underlying agreement entered with Bureau Veritas.

As part of Bureau Veritas policies, Bureau Veritas holds the right to audit the Third Parties' compliance with security provisions they indicate in the SIP.

REVIEW OF THIRD PARTY

Bureau Veritas conducts regular assessment of its Third Parties. Subsequently, a regular review of the SIP will be carried out at most once a year.

The Third Party will be kindly asked to update the present document, provide updated support document and inform Bureau Veritas of any change impacting its security stance or its ability to safeguard Bureau Veritas Data.

Date of last review	

SECURITY REQUIREMENTS

INFORMATION SECURITY ORGANISATION & POLICY

ORGANISATION OF INFORMATION SECURITY	
The Third Party shall have an identified employee responsible for overall management of information security.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

INFORMATION SECURITY POLICY	
The Third Party shall formalize an Information Security Policy. The policy shall address precise governance principles and fundamental security requirements to be adopted in order to provide a secure service. The policy shall be communicated to relevant parties and updated regularly.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

THIRD PARTY'S CERTIFICATION	
The Third Party shall: ▪ Inform Bureau Veritas of any certificates or proofs of compliance with one or several information security standards (e.g. ISO, NIST, etc.); ▪ Describe the certificates scope; ▪ Share with Bureau Veritas the certificates or any other proof of compliance.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

SUBCONTRACTING	
The Third Party shall identify and share the list of subcontractors who support in providing services to Bureau Veritas. Third party shall, through a formal process, evaluate and ensure that subcontractors handling Bureau Veritas information comply with the same security requirements as the Third party does.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

ADDITIONAL PRIVACY AND SECURITY PROVISIONS	
The Third Party shall communicate to Bureau Veritas the necessary documents and proofs (e.g. security audit report, vulnerability scans, etc.) demonstrating that security requirements and issues are adequately addressed. The Third Party shall provide Bureau Veritas with necessary information and access to perform a security audit if no recent audit report is provided by the Third Party.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

HUMAN RESOURCES

SECURITY TRAINING AND AWARENESS	
The Third Party shall ensure his employees who would intervene on Bureau Veritas premises or manipulate Bureau Veritas Data are trained to comply with the security requirements and best practices. The Third Party shall share evidences showing that their company maintains regular awareness raising actions and campaigns.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

RESPECT OF BUREAU VERITAS POLICIES	
The Third Party employees having access to Bureau Veritas systems and infrastructure shall acknowledge and accept to use Bureau Veritas resources with respect to Bureau Veritas policies and controls of this document.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

LOGICAL ACCESS

LOGICAL ACCESS TO IT RESOURCES AND DATA	
The Third Party shall maintain adequate security measures to protect against unlawful and unauthorized access to Bureau Veritas Data, resources used to provide the service to or collaborate with Bureau Veritas. These measures shall include (but not limited to): ▪ Using nominative accounts; ▪ Granting access rights based on the need-to-know principal; ▪ Individual authentication methods must be used to validate identity of users; ▪ Enforce a strong password policy; ▪ Review access rights regularly.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

PRIVILEGED ACCOUNT MANAGEMENT	
The Third Party shall manage privileged accounts having access to Bureau Veritas Data and tightly monitor their activity. Authentication method adopted for privileged accounts shall be stronger compared to regular accounts (e.g. use of Multi-Factor Authentication, stronger password policy, etc.).	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

AUTHENTICATION SYSTEM	
Access to Third Party's services and systems for Bureau Veritas employees shall go through the corporate directory, using a Single Sign-On (SSO) between Bureau Veritas and the Third Party. If not possible, the Third Party shall help Bureau Veritas draft an account management procedure that describes (but not limited to): ▪ Creation of accounts; ▪ Password policy; ▪ Initial password communication; ▪ Assigning/ modification/ deletion of authorizations.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

INFRASTRUCTURE, NETWORK AND SYSTEMS SECURITY

PROTECTION MEASURES	
The Third Party shall implement sufficient technical and organizational measures, to protect resources used to provide the service to Bureau Veritas and equipment hosting / manipulating Bureau Veritas Data. The following measures shall be considered: ▪ Proper segmentation of the network; ▪ Deploying firewalls to protect different networks and resources; ▪ Implementing a Host Intrusion Detection and Prevention product on hosts and monitoring alerts actively; ▪ Hardening servers hosting Data and applications; ▪ Protect servers using regularly updated anti-virus software or Operating System ("OS") appropriate countermeasures against viruses; ▪ Ensure OSs are maintained and updated as well as the applications installed on them; ▪ Regular scanning of network and hosts to detect any unauthorized or vulnerable configurations (Vulnerability scanning); ▪ Implementing and maintaining web filtering and email protection technologies.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

END POINT PROTECTION	
The Third Party shall implement sufficient technical and organizational measures, to secure employees workstations, laptops and other devices they use to fulfil their missions. The following measures shall be considered: ▪ Using updated and properly configured Operating Systems (“OS”); ▪ Protect end devices using anti-virus and anti-malware products and regularly update them; ▪ Ensuring anti-virus and anti-malware solutions are never deactivated on end devices, unless necessary; ▪ Ensuring access to devices is protected (e.g. by individual password); ▪ Implementing and maintaining web filtering and email protection technologies.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

MONITORING AND LOGGING

CONTINUOUS MONITORING AND LOGGING	
The Third Party shall have measures in place to continuously monitor and record any security events (e.g. attempted unauthorized access) on Bureau Veritas Data, as well as infrastructure and systems used in the scope of the contract. Level of recorded logs shall ensure accountability for performed actions and access to Bureau Veritas Data. Bureau Veritas shall be allowed to request logs of access to its Data. These logs shall be used for investigation purposes. The Third Party shall share the modalities through which Bureau Veritas can request Logs.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

CONTINUOUS MONITORING AND LOGGING	
The Third Party shall continuously correlate and analyze logs to detect security incident, data leakages or any events that would compromise security of Data and services.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

SECURE DEVELOPMENT AND MAINTENANCE

SECURE DEVELOPMENT	
The Third Party shall respect secure development practices when developing applications on behalf of Bureau Veritas. These practices of secure development shall take into account recommendations of acclaimed references (e.g. OWASP).	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

OPERATIONAL DOCUMENTATION	
The Third Party shall maintain and update regularly adequate and sufficient documentation of the application and services. Elements of the documentation shall be agreed upon with Bureau Veritas. Following elements shall be considered: ▪ Architecture diagram; ▪ Network flows; ▪ List of Production and Pre-Production environments, their purpose and security measures applied to protect them; ▪ Functional and technical patching cycles; ▪ Operational documentation for handling of the application. Bureau Veritas shall require copies of the documentation regularly.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

PHYSICAL AND ENVIRONMENTAL SECURITY

PHYSICAL AND ENVIRONMENTAL SECURITY CONTROLS	
The Third Party shall implement sufficient measures and controls to protect physical security of facilities hosting Bureau Veritas Data. These measures and controls shall safeguard the Third Party premises against unauthorized access as well as external and environmental threats. Following measures shall be considered: ▪ Gates giving access to private areas and areas hosting Data locked; ▪ Limit access only to authorized employees; ▪ Protection against intrusion (alarms and video surveillance, intrusion detection system, guards); ▪ Enforced measures to control access to the server rooms (individual access controls); ▪ Visitors identified and accompanied during their visits; ▪ Procedures in place to ensure that environmental issues (flood, fire, earthquakes, etc.) do not cause a disruption in service or loss of Data.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

PROTECTION OF BUREAU VERITAS DATA

DATA LOCATION AND ACCESS	
The Third Party shall define the geographical location of its datacentres or its cloud Third Party (i.e.: AWS) where Bureau Veritas Data would be stored. The Third Party shall be able to individually identify employees and machines having access to Bureau Veritas Data.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

DATA BACKUPS	
The Third Party shall formalize a backup procedure and test it regularly. Bureau Veritas Data shall be backed up. Retention and backup rules shall be defined with Bureau Veritas representative if necessary, in order to meet the business needs. Backups shall be replicated on a secondary site. All the Data Shall be stored, backed-up and purged in accordance with the applicable data protection laws and regulations and the contractual obligations.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

DATA ENCRYPTION	
The Third Party shall ensure Bureau Veritas Data is protected against unauthorized access. Data encryption shall be performed when requested by Bureau Veritas. The Third Party undertakes to encrypt Bureau Veritas Data in transit on external public networks, including the internet. The Data exchanges shall be performed using properly configured and secure protocols (SFTP, TLS). Additionally, encryption shall be deployed on computers and end devices containing Bureau Veritas' sensitive Data.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

DATA DESTRUCTION	
The Third Party shall formalize a Data destruction procedure for final Data destruction upon contract expiration or termination and Bureau Veritas' consent. The destruction procedure shall ensure Bureau Veritas Data cannot be recovered by any Third Party after final deletion.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

SECURITY INCIDENT MANAGEMENT

INCIDENT MANAGEMENT PROCESS	
The Third Party shall implement a security incident response process, as well as mechanisms to share information during and after an incident. The Third Party shall describe: ▪ The scope of information security incident that they will report to Bureau Veritas; ▪ The level of information disclosed to Bureau Veritas; ▪ Time window for reporting the security incidents; ▪ The notification procedure; ▪ Specific contacts information; ▪ Existing solutions that may apply in some security incident cases. The incident management process shall respect applicable laws and regulations (e.g. notification to local authorities delay).	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

INCIDENTS REPORTING	
The Third Party and Bureau Veritas shall agree on mechanisms and communication channels enabling: ▪ Bureau Veritas to report information security events it has detected to the Third Party; ▪ The Third Party to report information security events it has detected to Bureau Veritas; ▪ Bureau Veritas to track the status of a reported information security event.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

SERVICE LEVEL AND CONTINUITY

BUSINESS CONTINUITY PLAN	
The Third Party shall formalize a business continuity plan to ensure continuity of service provided to Bureau Veritas during an adverse situation, in adequacy with the service level defined in the contract (SLAs).	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

COMPLIANCE

GDPR COMPLIANCE	
The Third Party shall comply with applicable personal data protection laws and regulations, including the GDPR. In particular, the Third Party shall implement appropriate technical and organisational measures to protect Bureau Veritas Data including Personal data.	☐ Compliant ☐ Partially Compliant ☐ Not Compliant ☐ Not Applicable
Third Party comments:	

Glossary

CISO means Chief Information Security Officer.

Data (or Bureau Veritas Data) means the data, files and content belonging to Bureau Veritas, including Personal Data.

GDPR means the EU 2016/679 General Data Protection Regulation of 27 April 2016. The regulation aims to ensure protection of natural persons with regard to the processing of personal data and on the free movement of such data.

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.

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.

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.

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.

Third Party means any party not belonging to the Bureau Veritas' group, including but not limited to service providers, partners, subcontractors or clients.

Approvers

Name	Position	Date
Julien ANICOTTE	Group CISO	13/10/2020
Sonia DELPY	Group DPO	13/10/2020

Versions

Version	Author	Nature of the modifications	Date
1.0	Meryem OUKEMENI	Validation & Diffusion	27/07/2018
2.0	Youness TASTIFT	Revision of the SIP	09/10/2020