Cybersecurity Requirements for Suppliers

Purpose

These Cybersecurity Requirements establish the minimum controls that Suppliers must implement to protect Company Data and Company Systems and to support the confidentiality, integrity, availability, authenticity, regulatory compliance and operational resilience of the products and Services provided to the Company.
The document also defines the Supplier's responsibilities for cybersecurity governance, risk management, access control, data protection, secure development and maintenance, vulnerability and incident management, business continuity, subcontractor oversight, assurance, remediation and secure service termination. These requirements supplement the applicable agreement, statement of work, security schedule, data processing agreement and quality agreement; where requirements differ, the stricter requirement applies unless prohibited by law or expressly agreed otherwise in writing.

Scope

These requirements generally apply to all Suppliers and are mandatory for the following Supplier categories:

- Suppliers that access, process, store, transmit, host, support, develop, maintain, secure or otherwise handle Company Data, including personal, confidential, regulated or operational data.
- Suppliers that connect to, integrate with, administer, monitor, operate, support or maintain Company Systems, network and information systems, cloud environments, applications, infrastructure, devices or operational technology environments.
- Suppliers providing IT, OT, cybersecurity, cloud, hosting, data-center, managed-service, managed-security, telecommunications, network, software, hardware, digital, system-integration, development, maintenance or technical-support services.
- Suppliers with physical, logical, remote, administrative, privileged or emergency access to Company Data, Company Systems, restricted areas, service environments or critical operational sites.
- Suppliers whose failure, compromise, unavailability, performance degradation or loss of support may affect service continuity, business operations, regulatory obligations, cybersecurity posture, operational resilience or the availability, integrity, confidentiality or authenticity of Company Data or Company Systems.
- Suppliers involved in regulated, validated, GxP, manufacturing, laboratory, clinical, OT, safety-relevant or business-critical processes where cybersecurity weaknesses may affect compliance, operational integrity or continuity.
- Suppliers that develop, configure, customize, integrate, test, deploy, update or maintain software, firmware, automation, interfaces, scripts, APIs, infrastructure-as-code or digital components used by or for the Company.
- Suppliers that provide backup, disaster recovery, business continuity, monitoring, logging, identity, access-management, vulnerability-management, incident-response, security-testing or assurance services.
- Subcontractors, sub-suppliers and fourth parties used to deliver in-scope products or services, where their activities, access, dependencies or failures may create cybersecurity, data-protection, continuity or compliance exposure for the Company.

For all other Supplier categories not listed above, the requirements in §1 apply.

	Signature	Date	To be Revised within
Effective by	*Electronically signed-off by Maria Tarala*	19-Oct-2026	Three years
Validity Extended by			

Changes vs previous version

NA. First issue.

Table of Contents

Glossary 4
1 Limited baseline obligations applicable to all suppliers 5
2 Supply-Chain Cybersecurity Requirements Coverage 5
3 Supplier Cybersecurity Requirements 6
4 Assurance, Audit and Evidence 11
5 Security Exceptions, Non-Conformities and Remediation 12
6 Exit, Transition, Return and Deletion of Data 12
7 Compliance Monitoring, Enforcement and Remedies 12
8 History of Changes 13

Glossary

ACRONYM/TERMS	DESCRIPTION/DEFINITION
ACN	Agenzia per la Cybersicurezza Nazionale (Italian National Cybersecurity Agency).
API	Application Programming Interface; in the document template's manufacturer classification.
Asset	is a major application, general support system, high impact program, mission critical system, equipment, or a logically related group of systems.
Company	The Bracco legal entity identified in the applicable agreement, together with authorized affiliates where stated.
Company Data	Information provided by, collected for, generated for or otherwise processed on behalf of the Company, including personal, confidential, regulated and operational data.
Company Systems	Systems, applications, networks, devices, cloud resources, OT assets and interfaces owned, operated by the Company.
Guideline	is a recommended practice giving an overview of a business process that may involve more than one department or more than one business unit. It is usually addressed to those who have responsibility for the activities of the described process.
GxP	Good Practice requirements applicable to regulated activities, such as Good Manufacturing Practice, Good Laboratory Practice and Good Clinical Practice.
ITS	Information Technology Services.
MFA	Multi-Factor Authentication.
NIS	Network and Information Systems.
OT	Operational Technology.
RPO	Recovery Point Objective: the maximum acceptable amount of data loss measured in time.
RTO	Recovery Time Objective: the maximum acceptable time to restore a service after disruption.
SLA	Service Level Agreement.

1 Limited baseline obligations applicable to all suppliers

- Protect any Company information received during the relationship and use it only for authorized business purposes.
- Do not access, store, copy, transfer or disclose Company Data unless expressly authorized by the Company or required by the applicable agreement.
- Immediately notify the Company of any actual or suspected unauthorized access, disclosure, loss, theft, compromise or misuse of Company information, credentials, assets or materials.
- Use only approved communication channels and protect exchanged information against unauthorized access, alteration and disclosure.
- Use MFA for any remote, administrative, privileged or cloud access to Company Data, Company Systems or environments used to deliver the supply.
- Ensure that personnel involved in the supply receive appropriate cybersecurity awareness training and are informed of confidentiality, acceptable-use and security obligations relevant to their activities.
- Return or securely delete Company information, credentials, materials and assets when no longer required or upon Company request, unless retention is legally required.
- Do not appoint subcontractors to handle Company information or perform activities with cybersecurity relevance unless permitted by the applicable agreement or authorized by the Company.
- Promptly inform the Company if the supply scope changes in a way that may create access to Company Data, Company Systems, networks, operational technology, regulated processes or service continuity impact.

2 Supply-Chain Cybersecurity Requirements Coverage

These Cybersecurity Requirements are intended to cover the supply-chain security domains relating to supplier reliability, roles and responsibilities, personnel reliability, security compliance and audit, vulnerability management, business continuity and disaster recovery, identity and access management, physical security, personnel awareness, data security, network and communication protection, security-event monitoring, incident management and reporting, secure development and security by design and by default, ordinary and evolutionary maintenance including security updates, supply termination including return and deletion of data, and subcontracting or sub-supply obligations along the supply chain.

3 Supplier Cybersecurity Requirements

The following sections set out the operational cybersecurity requirements applicable to in-scope Suppliers.

3.1 Governance, Accountability, Roles and Compliance

- Maintain documented cybersecurity policies, standards, procedures and governance proportionate to the nature of the Services.
- Assign accountable personnel with sufficient authority, competence and resources to manage cybersecurity.
- Define and document the roles, responsibilities, interfaces and escalation points applicable to the Services, including security, continuity, incident management, maintenance, subcontractor oversight and regulatory support responsibilities.
- Identify and comply with applicable cybersecurity requirements.
- Maintain a process to monitor material changes in legal, regulatory, threat and technology conditions affecting the Services.
- Provide a current cybersecurity contact and escalation path to the Company.
- Promptly disclose any actual or potential conflict that could impair the Supplier's ability to meet these Cybersecurity Requirements.
- Support the Company's supplier qualification, risk classification and assurance activities by providing truthful and complete information on cybersecurity practices, known specific vulnerabilities, product and service quality, support and maintenance capacity, supply continuity, critical dependencies and relevant supply-chain risk assessments where applicable.

3.2 Cybersecurity Risk Management

- Maintain a documented risk-management process covering threat identification, vulnerability assessment, likelihood, impact, treatment, residual risk and ongoing monitoring.
- Assess risks before introducing or materially changing technologies, locations, connectivity, access models, subprocessors or delivery arrangements affecting the Services.
- Consider concentration risk, non-fungibility, single points of failure, geopolitical exposure and dependency on critical subcontractors.
- Document risk-treatment actions, owners, target dates, compensating controls and risk acceptance.
- Provide relevant risk information to the Company upon reasonable request, subject to appropriate confidentiality controls.

3.3 Asset, Configuration and Change Management

- Maintain an accurate inventory of hardware, software, cloud resources, interfaces, accounts, certificates, data stores, components and dependencies supporting the Services.
- Assign ownership and criticality to in-scope assets.
- Establish secure configuration baselines and hardening standards.
- Control, test, approve and document changes before production implementation.
- Perform security impact assessment for material changes and notify the Company when such changes may affect agreed security, compliance, availability or data-processing conditions.
- Remove or securely decommission unsupported, obsolete or unnecessary assets and services.

3.4 Identity and Access Management

- Apply least privilege, need-to-know, role-based access and segregation of duties.
- Use unique user identities and prohibit shared accounts unless technically unavoidable, formally approved, time limited and fully attributable.
- Implement MFA for all privileged, administrative, remote, third-party and cloud access to Company Data, Company Systems and service environments.
- Manage joiner, mover and leaver activities promptly and retain evidence of approvals.
- Review user and privileged access periodically and after material role changes.
- Restrict and monitor service accounts, emergency accounts and machine identities; rotate credentials and secrets appropriately.
- Use Company-approved secure remote-access methods and prohibit unauthorized persistent connectivity.
- Immediately revoke access when no longer required or upon Company instruction.

3.5 Data Protection, Privacy and Cryptography

- Process Company Data only for authorized purposes, in documented locations and only on documented instructions from the Company and the applicable agreement including with regard to transfers of Company Data.
- Ensure that persons authorized to process Company Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- Classify and handle Company Data according to its sensitivity and applicable legal or contractual requirements.
- Engage another processor only with prior written authorization of the Company.
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk pursuant to any applicable data protection laws including inter alia encryption of Company Data in transit using current secure protocols and encryption of data at rest.
- Protect cryptographic keys and secrets throughout their lifecycle, including generation, storage, rotation, backup, revocation and destruction.

- Apply data minimization, retention and secure-deletion controls.
- Prevent unauthorized copying, downloading, transfer, commingling or use of Company Data.
- Support data-subject, legal-hold, investigation, portability, return and deletion obligations where applicable.

3.6 Network, Infrastructure, Endpoint and Cloud Security

- Segment environments and restrict network flows according to business need and risk.
- Deploy and maintain anti-malware, endpoint detection, host firewall, secure configuration and device-management controls appropriate to the Services.
- Protect internet-facing services through layered controls and monitor them for attack and abuse.
- Secure administrative interfaces and management planes; do not expose them directly to the internet unless specifically protected and justified.
- Maintain secure tenant, account, logging, encryption, resilience and access configurations for cloud services.
- Separate development, test and production environments and restrict use of production data outside production.
- Apply secure wireless, mobile and removable-media controls where applicable.
- Protect communications used for the Services through appropriate encryption, integrity, routing, filtering, remote-access and network-security controls.

3.7 Vulnerability, Patch and Security Testing

- Maintain continuous processes to identify, assess, prioritize, remediate and verify vulnerabilities affecting the Services.
- Monitor relevant vulnerability sources, supplier advisories, threat intelligence and exploited-vulnerability information.
- Perform authenticated vulnerability scanning at a risk-based frequency and after material changes.
- Apply security patches within documented risk-based timeframes; expedite remediation for actively exploited or critical vulnerabilities.
- Implement documented compensating controls where remediation cannot be completed promptly.
- Perform penetration testing or equivalent independent security testing for high-risk or internet-facing services at a risk-based frequency.
- Notify the Company of material vulnerabilities that may affect Company Data, Company Systems or service continuity and communicate mitigation and remediation status.
- Prohibit security testing against Company Systems without prior written authorization.

3.8 Secure Acquisition, Development, Maintenance and Security by Design

- Apply a secure development lifecycle when developing, configuring, integrating or maintaining software for the Company.
- Apply security-by-design and security-by-default principles so that products and services are designed, configured and delivered with protective settings enabled by default, unnecessary functions disabled and security risks considered from inception.
- Conduct code review and appropriate static, dynamic, dependency, container and infrastructure-as-code security testing.
- Separate development, test and production duties and environments.
- Manage open-source and third-party components, including license, provenance, vulnerability and end-of-support risks.
- Maintain processes for vulnerability disclosure, corrective releases and supported product lifecycles.
- Provide ordinary and evolutionary maintenance, including security updates, corrective releases and supported upgrade or migration paths, for the agreed lifecycle of the Services.
- Define support and maintenance commitments for material Services, including supported versions, security patch timelines by severity, end-of-support notice periods, upgrade responsibilities and mitigation measures where updates cannot be applied promptly.
- Do not introduce hidden functionality, unauthorized remote access, malicious code or intentionally weakened security controls.

3.9 Logging, Monitoring and Detection

- Generate logs sufficient to support security monitoring, accountability, investigation and regulatory or contractual obligations and retain them for at least six months for material Services, or longer where required by law, contract, risk assessment or Company instruction.
- Monitor and escalate security alerts affecting Company Data, Company Systems or the Services without undue delay and in accordance with the agreed incident-notification process.

3.10 Cybersecurity Incident Management and Notification

- Maintain documented incident-response plans, roles, communication paths, evidence-preservation procedures and decision criteria.
- Train relevant personnel and test incident-response arrangements periodically.
- Notify the Company without undue delay after becoming aware of a Cybersecurity Incident or material security event that affects, or could reasonably affect, Company Data, Company Systems or the Services.
- Classify incidents by severity, notify the Company without undue delay, and provide periodic updates until containment, recovery and closure.

3.11 Business Continuity, Backup and Disaster Recovery

- Maintain documented business-continuity and disaster-recovery arrangements appropriate to Services.
- Comply with the Services' RTO and RPO and SLA.
- Maintain protected, monitored and recoverable backups for systems and data necessary to deliver the Services.
- Protect backups from unauthorized alteration or deletion and maintain offline or immutable capability.
- Test restoration and recovery procedures of the delivered Services at least annually and remediate identified weaknesses.
- Perform continuity and disaster-recovery tests at least annually for the Services, or more frequently where required by contract, risk or regulation, and provide evidence of scope, results, deviations and remediation actions upon request.
- Notify the Company of material continuity risks, test failures and invocation of continuity arrangements affecting the Services.

3.12 Personnel Security, Reliability, Awareness and Acceptable Use

- Apply risk-based personnel reliability controls, including pre-employment or pre-engagement screening where lawful and appropriate, for personnel who access Company Data, Company Systems or critical service environments.
- For personnel assigned to high-risk or privileged activities, obtain confidentiality commitments, verify identity and qualifications, confirm completion of required security training, and maintain evidence of authorization before granting access.
- Provide cybersecurity and privacy training to personnel involved in the Services at onboarding and periodically thereafter, with role-specific training for privileged users, developers, administrators, support personnel and incident responders.
- Maintain disciplinary processes for security violations, subject to applicable law.
- Promptly remove access and recover Company assets when personnel leave or change roles.
- Use Company Data and Company Systems only for authorized business purposes.

3.13 Physical and Environmental Security

- Control physical access to facilities and areas hosting systems or media supporting the Services.
- Maintain visitor management, access records and monitoring appropriate to risk.
- Protect any equipment supporting your service against theft, tampering, fire, water, power disruption and environmental hazards.
- Securely transport, store, reuse and dispose of media and equipment containing Company Data.

3.14 Subcontractor, Sub-Supplier and Fourth-Party Security

- Perform due diligence before appointing subcontractors that may affect Company Data, Company Systems or the Services.
- Maintain a current list of material subcontractors and service locations.
- Obtain prior written authorization from the Company, or provide prior notification where contractually permitted, before appointing or materially changing subcontractors that may process Company Data, access Company Systems or critical service environments.
- Flow down equivalent security, confidentiality, incident-notification, audit, resilience, data-protection, return and deletion obligations.
- Monitor material subcontractors on an ongoing risk-based basis and maintain evidence of due diligence, contractual flow-down, security performance, incident reporting and remediation follow-up.
- Remain fully accountable for subcontractor acts and omissions.
- Notify the Company of subcontractor incidents, failures, ownership changes or concentration risks.

3.15 Operational Technology and Product Security

- Apply security controls appropriate to safety-critical, manufacturing, laboratory and OT environments.
- Avoid uncontrolled direct internet connectivity to OT assets.
- Use approved, monitored and time-bound remote access with MFA and session accountability.
- Maintain asset, firmware, software and support-lifecycle information.
- Coordinate vulnerability remediation, patching and compensating controls to protect both cybersecurity and operational safety or validated state.
- Protect engineering workstations, configuration files, recipes, logic, backups and portable media.
- Provide secure-by-default configurations, hardening guidance and vulnerability-notification channels for supplied products.
- Support recovery, replacement and transition where a product reaches end of support.

4 Assurance, Audit and Evidence

- Complete Company security questionnaires accurately and within the requested timeframe.
- Provide reasonable evidence, which may include policies, certifications, independent assurance reports, penetration-test summaries, recovery-test evidence, access reviews, architecture information and remediation plans.
- Provide assurance evidence at onboarding, upon material change, after significant incidents and periodically thereafter, with timing, scope, remediation deadlines and escalation based on risk and contractual obligations.

- Promptly correct inaccurate or incomplete information previously provided.
- Track findings to closure and provide status updates and evidence of remediation.
- Ensure certifications and assurance reports are relevant to the Services and current; certification does not replace compliance with these Cybersecurity Requirements.

5 Security Exceptions, Non-Conformities and Remediation

- Promptly disclose any inability to comply with an applicable requirement.
- Submit a documented exception request describing the requirement, rationale, affected scope, risk, compensating controls, owner and proposed expiry date.
- Do not treat silence or continued service as approval of an exception.
- Implement corrective actions within agreed timeframes.
- Reassess exceptions after material change and before expiry.
- Accept that unresolved material non-conformity may result in restricted access, enhanced oversight, suspension, disqualification or contractual remedies.

6 Exit, Transition, Return and Deletion of Data

- Support an orderly exit, transition or termination of the Services without compromising security, continuity, integrity, availability or regulatory obligations.
- Return Company Data and Company-provided materials in an agreed format, within agreed timelines and through secure transfer methods.
- At the choice of the Company, delete or return all the Company Data to the Company after the end of the provision of services relating to processing, and delete existing copies unless applicable law or the agreement require storage of the Company Data.
- Provide written confirmation of return, deletion, decommissioning or continued lawful retention when requested by the Company.
- Apply documented secure-deletion methods proportionate to the data and media type, address backups and replicated data, complete deletion within agreed timelines, and provide a deletion certificate or equivalent written attestation when requested.
- Revoke access, terminate connectivity, remove Company configurations and protect residual information during and after transition.

7 Compliance Monitoring, Enforcement and Remedies

- The Company may request corrective action, additional controls, independent assurance, enhanced monitoring or risk treatment in response to identified risk.
- Non-compliance may lead to suspension of access or Services, escalation, removal from an approved supplier list, termination or other remedies available under the agreement or law.

- Exercise of assurance or enforcement rights does not transfer Supplier responsibility to the Company.

8 History of Changes

Previous Version	Effective Date	Reason(s) for Change
NA	NA	NA

Author(s):

Name	Function	Signature	Date
Maria Tarala	ITS-Global Complinace Manager	*Electronically signed-off*	*16-Oct-2026*

Reviewed by:

Name	Function	Signature	Date
Gianluigi Meggiorin	ITS-Global Cyber Security Manager	*Electronically signed-off*	*16-Oct-2026*

Approval :

Name	Function	Signature	Date
Andrea Provini	ITS-Chief Information Officer	*Electronically signed-off*	*19-Oct-2026*