BASF Group

Cyber Security Addendum

Corporate Development

Table of Contents

1. Purpose and Scope

This document defines specific requirements to be fulfilled by each supplier which has access to or managing BASF's information assets. Following the international standard ISO/IEC 27001:2013 and best practices, this Cyber Security Addendum document defines globally binding controls that cover the supplier's responsibilities for BASF's information assets.

Thus, the purpose of this document is the definition of specific controls that must be implemented and a consistent and effective approach for appropriately protecting BASF's information assets against e.g. access by unauthorized persons, loss or non-availability, manipulation of falsification.

The Cyber Security Addendum provides a reusable set of security and compliance requirements that have to be provided to all external partners and contractors having access to or managing BASF's information assets. and as such pose information security risk to BASF.

2. Definitions

Term	Definition	Examples
Asset	Assets are all resources related to information or information processing that have value to BASF. The term “asset” comprises technical assets and non-technical, organizational assets as well as information assets	Technical, non-technical, organizational and information assets
Information Asset	Data or other knowledge that has value to the organization	Patent, chemical formulation, client relations, business processes
Supplier / Contractor	An organization or an individual that provides a product of service to BASF within a contractual agreement. Other terms commonly used for supplier are contractor, producer, provider, seller, or vendor.	Microsoft, SAP, Salesforce
Risk Assessment	Identify and assess existing security risk as necessary and maintain the security risk register Review supplier’s documentation (e.g. high-level proposed design, external assessments)	Architecture review of the entire solution with all connected interfaces Review of the provided documentation specially regarding solution design and IT-Security measures Technical Risk Assessment including testing of systems and components in scope Review of the provided SOC 2 Type 2 reports for critical BASF systems

3. Addendum

3.1 General

The contractor must ensure compliance with these requirements by itself, its employees, and their involved (sub-)contractors who are needed to deliver the service for BASF. The contractor agrees to process or use the data and programs provided or made available by BASF solely to the extent required to fulfill its contractual obligations to BASF.

All data, information and knowledge gained under, through or by any means related to performance of contractual obligation to or for BASF must be handled compliant with applicable BASF "Classification of Information" schemes, but in any case, at least following industry best practices from frameworks such as ISO 27001, as such maybe amended or updated, to ensure confidentiality, integrity and availability of BASF data and contractor's ability to perform its obligations to or for BASF. BASF must be immediately informed, if any compromise of information assets (BASF's or otherwise) is detected or there are any circumstances that could affect contractor's ability to perform its obligations to or for BASF. The requirements provided herein also apply to any contractor's subcontractor of any tier and contractor must affirmatively require each such subcontractor to bind themselves to these requirements as if they were contractor.

The contractor and its subcontractors should, at a minimum, review the Cyber Security Addendum on an annual basis unless specifically requested otherwise below.

Note:

Chapters 3.2 to 3.4 are valid for any kind of services provided to BASF independent of the service model. Chapters 3.6 – 3.10 are valid for On-Premise or Infrastructure-as-a-Service (IaaS) services.

If confidential or strictly confidential BASF data is processed chapter 3.5 must also be considered.

3.2 Access Control

When contractor's employees need access to BASF data or information, and/or applications handling BASF data or connected to BASF, the following principles must be followed:

- Contractor must have and maintain a documented access management process for granting, modifying, and removing user access as well as defining requirements for role concepts, privileged user access, and access record keeping.
- A review of digital identities on a periodic basis as appropriate, but in any case, at least annually.

- Contractor must have means and methods for granting of access rights to persons on a need-to-have principle and immediate revoking access when such need is no longer required.

If access to BASF assets is necessary, the following additional principles must be followed:

- Each person granted or having access must have a distinct user identification (UserID) and password or authentication token that must be entered into prior to gaining access BASF IT systems, BASF data or information, and/or applications handling BASF data or connected to BASF.
- Contractor must have means and methods to provide prompt identification and notification of the expiration of an UserID in the event of a role transfer or termination of an employee, contractor or subcontractor.

3.3 Management of Contractor Employees and Personnel Accessing BASF Resources and Information

Contractor must have in place the noted means and methods concerning training of all contractor employees or personnel granted or having access to BASF data or information, and/or applications handling BASF data or connected to BASF provided below:

- an appropriate use policy covering the acceptable use of information, devices, and technology;
- means and methods for recording and storing confirmation in writing from each person accessing of their acknowledgement and understanding of Contractor's acceptable use policy.
- a program for communicating and training the importance of information protection, the overriding need for personal responsibility, reporting security risks and incidents, and the type(s) of protection required for different data classification levels.
- periodic review to stay aligned with policies, standards and procedures as well as with business requirements.
- means and methods of monitoring and assuring compliance and currency of all individuals with latest policies, standards and procedures as well as with business requirements, retraining and retesting and communicating to affected individuals and their management any such non-compliance.

3.4 Information Protection on Applications and Systems

When the Contractor provides services to BASF where BASF data is accessed, available, handled, processed, or stored, Contractor must have in place the below listed requirements which are following industry best practices from frameworks such as ISO 27001.

- Legal and Regulatory Requirements -–Implemented security controls must meet any regulatory and legal requirements relevant to the contractor agreement with BASF
- Policies and Procedures - Information Security Policies and/or Procedures must be implemented to regulate the processing of information assets
- Procedures for a Risk Management Methodology - Documented Risk Management Methodology and Procedures to cover the assessment, treatment, communication, and monitoring of security risks
- Data Privacy Breaches - Procedures for identifying, responding, and notifying BASF of a data privacy breach when the breach relates to the service provided to BASF. Protection requirements of the confidentiality of BASF data are defined within the specific contractor agreement
- An information classification scheme with defined processes and procedures for classifying IT assets
- Protection of Test Data - Separation of environments to restrict production data from being used in testing environments. If operational data containing PII or sensitive data is required, proper procedures and security controls must be established to appropriately sanitize, protect, and erase the data used at least in compliance with ISO27001 and IT cloud data processing industry leading practices, as either may change or evolve
- Separation of BASF Data – BASF data must be separated, either physical or logically, from the data of other clients
- Management of Removable Media - Defined policies and procedures for the use of removal media including the authorization of approved media and recording of removals
- Security Requirements to Protect Wireless Networks - Security controls to protect wireless network access through authentication, encryption and user level network access control technologies
- Data Disposal - Documented procedures for disposal of all documents and electronic media containing BASF’s information and/or BASF Data when no longer required.

Note:

BASF must be informed about the contact ways to the contractors SOC team before the service is taken into operation. Contact information can be communicated directly to the BASF Cybersecurity Defense Center via E-Mail (soc@basf.com)

- If data breaches happen BASF Cyber Security Defense Center must be contacted immediately. Upon demand breach relevant information must be shared with the BASF SOC team for forensic analysis

See BASF Cyber Security Defense Center (SOC / CSIRT) for details.

3.5 Processing of (Strictly) Confidential Data

If confidential or strictly confidential data will be processed the following additional security requirements must be fulfilled:

- Data at rest and in transit must be encrypted at any time using industry standard mechanisms
- BASF data must be fully isolated against any non-BASF data
- Multifactor authentication must be in place for users and administrators
- BASF must act as identity provider wherever applicable
- BASF standard authorization management solution must be used, in cases this is not possible an equivalent must be used
- Application log information must be shared with BASF upon demand. An interface to the BASF Security and Incident Management System (SIEM) must be implemented wherever applicable.
- A security incident process must be setup where the provider ensures that BASF will be informed immediately if a security incident appears (e.g. security breach concerning BASF data).
- Security Incident Management Assessment Procedures - The Incident Response Policy must include without limitation procedures to address the impact assessment of an incident type, remediation, and the post-incident analysis and communication and escalation processes regarding information security and reporting relevant incidents back to BASF.

Non-disclosure agreements must be implemented to ensure information protection wherever BASF confidential and strictly confidential information is being processed.

Single point of contact for these procedures have to be named with detailed contact information upfront. See BASF Cyber Security Defense Center (SOC / CSIRT) for details.

For suppliers managing or having access to BASF confidential or strictly confidential information of strategic relevance[1] additional information security requirements must be integrated during all stages of the relationship. This includes the following requirements:

a) Supplier verification must be performed to manage the geographic, political, legal and information security risks.
b) Reviews of supplier security posture (yearly security audit or SOC 2 Type 2 review) must be ensured.
c) BASF's right to audit supplier procedures and information security controls related to the agreement,
d) Service contracts must be reviewed at least annually.
e) Security roles and responsibilities must be defined (e.g. Information Security Manager, Risk Manager) for both, BASF and supplier side.
f) Supplier's obligation to provide reports of service delivery performance, information security activities and compliance with BASF's information security requirements,
g) Monitoring and reporting capabilities must be implemented to track key security metrics, such as number of information security incidents, types of attacks, targeted services etc.
h) KPI reports based on security incidents and remediation activities (e.g. response time) must be provided by the supplier on a regular basis.

3.6 Management of IT Systems

When the contractor manages an IT system where BASF data is handled, accessed, available, processed, or stored, the system must have in place at least following industry best practices from frameworks such as ISO 27.001:

- Incident Management Procedures - The Incident Management Policy and Procedures must include without limitation clear criteria for prioritizing and escalating incidents. The criteria should be reviewed at least annually.
- Change Management - A formal change management procedure.

[1] Strategic relevant implies a high (> 10 Mio) or very high (> 100 Mio) business impact due to loss of management control (incl. EHS impact) or impaired growth.

- Separation of Development, Testing & Operational Environments – This must include utilization of separate and distinct software environments with clear requirements for transferring or promoting from one to another.
- Secure Coding Requirements – This must include without limitation having secure coding specifications for each programming language and appropriate training provided to those developers.
- Configuration of Endpoints - This must include without limitation having secure baseline builds, configurations or the like to harden and manage all endpoints such as servers, laptops, and mobile devices. This would include restrictions for unauthorized applications, pre-configured systems with approved security software, and administrative design/tools for endpoints.
- Encryption of Endpoints - This must include without limitation full disk encryption utilized for all endpoints.
- Protection Against Malware – Such protection must apply without limitation to current versions of a virus protection system and anti-malware protection system with updated signature databases on each endpoint as any anti-malware updates become available.
- Controls Against Malware – This must include without limitation malware protection management program to install and configure malware protection software, keep malware protection software up to date, review effectiveness of protection software, reduce risks of malware being downloaded, and reporting/recovery activities regarding malware attacks.
- Cryptography Procedures - This must include without limitation procedures and means for documenting the use of cryptography for protecting the confidentiality, integrity and/or authenticity of BASF data.
- IT Asset Inventory Management - This must include without limitation an IT Asset Inventory Management Process to identify, maintain, and address required changes.
- Backup Procedure Requirements - These must include without limitation procedures and means for defining, performing and documenting the planning, scheduling, recording, labelling, verifying, retaining, protecting, and restoring of data to and from backups.
- Network Segregation Procedures - These must include without limitation proper network segregation procedures and means to incorporate the use of security domains (e.g. VLAN’s) and to isolate particular network traffic to prevent impact upon other network traffic.

- Security of Network Services - These must include without limitation procedures and means for managing network firewalls to filter malicious traffic, preventing unauthorized network traffic from gaining access to or leaving networks, identifying and mitigating DDoS attacks, and limiting information disclosure about networks at the network level.
- Removing or Disabling of External Connections - These must include without limitation procedures and means for removal and disabling of external connections that are unauthorized or no longer required.
- Technical Vulnerability Management - These must include without limitation procedures and means to scan, manage, and mitigate vulnerabilities across IT assets including Patch Management Procedures for regularly addressing known vulnerabilities.
- Scanning & Monitoring of Electronic Communications - These must include without limitation procedures and means for electronic message scanning for malware, phishing, chain letters, offensive content or accidental leakage of business information.
- Penetration and Vulnerability Testing - These must include without limitation procedures and means for penetration testing and vulnerability assessments performed on an annual basis.

Note:

If a security incident happens BASF Cyber Security Defense Center must be contacted immediately. See BASF Cyber Security Defense Center (SOC / CSIRT) for details.

3.7 Physical & Environment Security (on-premise scenarios only)

Contractor must have and use means and methods of physical security control for all data centers and office space used to provide services to, or for BASF involving BASF IT systems, BASF data or information, and/or applications handling BASF data or connected to any BASF IT network, node or the like.

3.8 Business Continuity and Disaster Recovery

Planning Information Security Continuity - Contractor must have and use means and methods for addressing the availability of Contractor information systems and infrastructure to meet the requirements defined in the contractor agreement.

Risk Assessment – Contractor must, upon the request of BASF, promptly complete a risk assessment for all assets within the scope of services to be or provided to BASF based on the importance of the assets to fulfilling the business objectives of BASF including the business impact analysis and the potential business consequences of a loss or compromise of the availability, confidentiality or integrity of the assets.

Note:

If a disaster happens BASF Cyber Security Defense Center must be contacted immediately. See BASF Cyber Security Defense Center (SOC / CSIRT) for details.

3.9 Modification of Access

Contractor understands and agrees that BASF may, as it deems appropriate, modify the type of access Contractor may have to BASF IT systems, BASF data or information, and/or applications handling BASF data or connected to BASF to accommodate technical and organizational requirements at any time.

3.10 Monitoring and Change of the Guidelines

BASF may audit Contractor's compliance on an annual basis with the obligations herein by providing contractor with prior notification. Such audit may be conducted wherever contractor or its subcontractor use, store, process or handle BASF information. The Contractor will provide cooperation and assistance to the designated BASF representative(s) involved in any such audit. Such cooperation must include without limitation providing BASF's representative access to all relevant operation premises, documentation, records, certifications, policies/procedures and other relevant information in any tangible form, and access to relevant Contractor and subcontractor employees and contractors sufficient to permit BASF to verify Contractor's compliance with its obligations hereunder. Contractor must require its contractors and subcontractors to comply with its obligations herein as if they were a party to this contract.

Further, BASF may modify the requirements herein from to time and must provide Contractor with either notice of or access to such requirements. Such requirements and modifications must be limited to those that BASF imposes on itself. BASF must have the right to subject Contractor's IT infrastructure connected, directly or indirectly, to BASF IT systems, BASF data or information, and/or applications handling BASF data.

4. Appendix

4.1 Classification of Information Scheme

This classification scheme is taken from the “Asset Management” BASF Corporate Requirement Document. The following classification scheme is used to derive the classification of IT Assets from the classification of the underlying information assets.

Information Class	Description
Public	Information that has already been published (e.g., on the Internet or in brochures) or released for publication by the responsible communication unit.
Internal	Information that is not intended to be released to the public, but which may be made known to all employees of BASF Group without causing any damage to BASF. If third parties need access to this information, a Non-Disclosure Agreement or similar legal contract is necessary.
Confidential	Information that may only be disclosed to a specific group of authorized persons in BASF. The group can consist of a substantial number of people. Disclosing the information to others than the authorized persons would cause damage to BASF. If third parties need access to this information, a Non-Disclosure Agreement or similar legal contract is necessary
Strictly Confidential	Information that represents the top business secrets of a division/business unit (and therefore of BASF), or due to regulatory constraints. Information that may only be disclosed to a very restricted and explicitly named circle of authorized persons in BASF. Disclosing the information to others than the authorized persons would cause business-critical damage to BASF. Disclosure/transfer of this information to a person other than the already authorized persons must be approved by the owner of the information. If, in exceptional cases, third parties need access to this information, a Nondisclosure Agreement or similar legal contract is necessary

4.2 BASF Cyber Security Defense Center (SOC / CSIRT)

The BASF’s Cyber Security Defense Center (CSDC) is organized in two major parts (SOC and CSIRT) and follows a multi-tier work sequence.

The Security Operations Center - SOC - (Tier-1) is in charge of security alert validation. The Global Computer Emergency Response Team (gCERT) is the CSIRT – acting as Tier-2 in the CSDC - and in charge of security incident management. The SOC has the ability to reach out the stand-by of the Tier-2 in case this is needed.

As the BASF global Computer Emergency Response Team is an accredited member of Forum of Incident Response and Security Teams (FIRST - https://www.first.org) BASF's main contacts and encryption details for relevant Cyber Security events, alerts, incidents our abuses are listed and continuously maintained on the following FIRST team's page:

https://www.first.org/members/teams/basf_gcert

The preferred communication channel is via encrypted email communication or in case of emergency also via the provided phone number. The necessary public key information for establishing a secure email communication can be found on the FIRST's team page.

Below please find some further details including the contact details of the SOC and the availability of each organization:

Organization	Role	Availability	Contact details	Secure communication
Security Operations Center (Tier-1)	SOC	24/7/365	E-Mail: soc@basf.com Phone: +49 621 60 50003	
Global Computer Emergency Response Team (Tier-2)	CSIRT	8/5 plus on-call exclusively *to be initiated by the SOC*	E-Mail: cert@basf.com	OpenPGP – see chapter 2.2

Contractor should fill out the template below with the details of his security organization and send them to the BASF Cyber Security Office mailbox

(security-consulting@basf.com).

Organization	Role	Availability	Contact details	Secure communication
Name of the team	*SOC or CSIRT*	*Time of availability (24/7 or 8/5 ..)*	*E-Mail addresses / telephone numbers etc.*	*Instructions for establishing a secure communication channel*