BASF Group

Cyber Security Addendum

Table of Contents

1. Disclaimer

The Security Addendum contains requirements for information security. All suppliers are required to fulfill the specifications in the "General" chapter. The other requirements are separated according to supplier type and should be fulfilled accordingly. An explanation of the supplier types can be found at the beginning of the respective chapter.
The requirements are divided into SHOULD and MUST. MUST requirements have to be fulfilled, if at least one of them is not implemented by the supplier, they are considered as showstoppers. Showstoppers are subject to a manual check by means of an interview with the service provider.
If evidence is required for individual controls, this must also be submitted.

2. General

General Supplier Security is relevant if risks apply regardless of the service provided

2.1 Single point of contact – Cyber security

A single point of contact for cyber security MUST be appointed.

Up-to-date contact information for the single point of contact for Cyber Security BASF MUST be provided on a regular basis.

Critical security requirement: The single point of contact for cyber security MUST be available outside normal business hours.

2.2 Personal Security

All employees involved in the delivery of the service MUST be sufficiently trained and aware of the information security topics.

There SHOULD be a current rights and roles concept in place to ensure that only authorized employees have access to the systems relevant to the service (need-to-know).

Cyber security training SHOULD be refreshed annually for all employees.

2.3 Information Security Management

A CISO MUST be appointed.

The organization SHOULD have an information security management system whose scope includes the service procured.

Critical security requirement: The organization MUST have a certified information security management system whose scope includes the service to be delivered.

2.4 Business Continuity Management

A business continuity manager SHOULD been appointed.

The organization SHOULD have a business continuity management system whose scope includes the service procured.

BCM exercises SHOULD be conducted at least annually.

All employees SHOULD be made aware of the importance and availability of BCM.

2.5 Supply Chain Security

There MUST be an up-to-date overview of all subcontractors relevant to the services provided.

2.6 Supplier Audits

All agreements SHOULD recorded and documented in written form.

Confirmations of agreements SHOULD be made required from the contract partner.

3. Consulting security

Consulting refers to the service provided by an individual with expert advice with respect to technology purchases, strategy decisions, system design and development, architecture, specifications and solutions to other technology-related challenges.

3.1 Resource Management

There MUST be an internal resource management system in place to ensure that all projects are adequately staffed with qualified personnel.

3.2 Handling of client information

There MUST be a standard process in place to ensure the confidentially of client information at all times before, during and after projects.

Critical security requirement: It MUST be ensured that confidential documents are not left unattended in unlocked offices.

3.3 Information validation

In the case of particular critical task, it SHOULD be ensured that these are always carried out via the dual control principle (e.g. preparation of final report).

It MUST be ensured that all information used in the course of the project are adequately validated by a standard process.

3.4 Data encryption

Standardized cryptographic procedures MUST be implemented and documented that ensure the confidentiality, integrity and authenticity of the transmitted data.

Critical security requirement: Data transfers MUST be classified into different data classification level.

3.5 Equipment handling

There MUST be a policy on the general handling of equipment.

There SHOULD be a policy on loss of equipment procedures.

There MUST be a security incident handling process in place to ensure that BASF is informed of potential consequences for the organization (e.g. in the event of theft of IT equipment on which BASF data is stored).

It SHOULD be possible to lock and delete stolen or lost devices remotely.

It SHOULD be ensured, that the hard drives of all end devices are encrypted.

3.6 Identity and access Management

It MUST be ensured via end-to-end identity and access management that only those employees have access to BASF data who actually need it for work on a given project (need-to-know).

It SHOULD be ensured via end-to-end identity and access management, that employees only have the necessary authorizations (least privilege).

There MUST be a defined process in place to ensure that personnel changes are reflected in the assigned roles and permissions (Joiner-Mover-Leaver process).

3.7 Software security

The IT management MUST ensure that only current software versions that are permissible in terms of cyber security best practices are used to process BASF data.

There SHOULD be a test environment in which software changes are tested previously to productive use.

3.8 Backups

Regular Back-Ups MUST be performed.

3.9 Malware protection

A policy to prevent malware MUST be in place.

Critical security requirement: The use of external removable media MUST be restricted.

3.10 Physical security

Rooms in which endpoint devices are stored SHOULD be lockable.

External persons SHOULD be accompanied by employees while they are on the company premises.

3.11 Compliance

A process to ensure that all applicable compliance requirements are met before, during and after a project MUST be in place.

3.12 Data Privacy

A data protection officer SHOULD been appointed.

The organization SHOULD have a comprehensive data privacy management system.

4. Service security

Service refers to all routine or periodic actions taken to assure the intended purpose of the product or system. This includes administration, support, maintenance, installation, repair or other measures.

4.1 Resource Management

There MUST be an internal resource management system in place to ensure that all services are adequately staffed with qualified personnel.

4.2 Handling of client information

There MUST be a standard process in place to ensure the confidentially of client information at all times before, during and after projects.

Critical security requirement: It MUST be ensured that confidential documents are not left unattended in unlocked offices.

4.3 Information validation

In the case of particular critical task, it SHOULD be ensured that these are always carried out via the dual control principle (e.g. preparation of final report).

It MUST be ensured that all information used in the course of the service are adequately validated by a standard process.

4.4 Data encryption

Standardized cryptographic procedures MUST be implemented and documented that ensure the confidentiality, integrity and authenticity of the transmitted data.

Critical security requirement: Data transfers MUST be classified into different data classification level.

4.5 Equipment handling

There MUST be a policy on the general handling of equipment.

There SHOULD be a policy on loss of equipment procedures.

There MUST be a security incident handling process in place to ensure that BASF is informed of potential consequences for the organization (e.g. in the event of theft of IT equipment on which BASF data is stored).

It SHOULD be possible to lock and delete stolen or lost devices remotely.

It SHOULD be ensured, that the hard drives of all end devices are encrypted.

4.6 Identity and access Management

It MUST be ensured via end-to-end identity and access management that only those employees have access to BASF data who actually need it for work on a given project (need-to-know).

It SHOULD be ensured via end-to-end identity and access management, that employees only have the necessary authorizations (least privilege).

There MUST be a defined process in place to ensure that personnel changes are reflected in the assigned roles and permissions (Joiner-Mover-Leaver process).

4.7 Software security

The IT management MUST ensure that only current software versions that are permissible in terms of cyber security best practices are used to process BASF data.

There SHOULD be a test environment in which software changes are tested previously to productive use.

4.8 Backups

Regular Back-Ups MUST be performed.

4.9 Malware protection

A policy to prevent malware MUST be in place.

Critical security requirement: The use of external removable media MUST be restricted.

4.10 Physical security

Rooms in which endpoint devices are stored SHOULD be lockable.

External persons SHOULD be accompanied by employees while they are on the company premises.

4.11 Compliance

A process to ensure that all applicable compliance requirements are met before, during and after a project MUST be in place.

4.12 Data Privacy

A data protection officer SHOULD been appointed.

The organization SHOULD have a comprehensive data privacy management system.

5. Hardware security

Hardware refers to the physical parts of a computer system and related devices including internal hardware devices (e.g., motherboards, RAM) and external hardware devices (e.g., monitors, mice, printers).

5.1 Delivery

It MUST be ensured throughout the packaging and transport route, that all equipment is adequately protected against damage and manipulation.

There SHOULD be a standardized process for recording, processing and closing out faulty deliveries.

5.2 Handling of client information

It MUST be ensured via end-to-end identity and access management, that only those employees have access to BASF data (incl. order data) who actually need it for their work (need-to-know).

It MUST be ensured, that all subcontractors involved in BASF orders must sign a non-disclosure agreement (NDA) before commencing the order.

5.3 Product Security

There SHOULD be a process in existence to ensure the functionality of distributed hardware (internally by the supplier or upstream by the manufacturer).

If hardware is to be implemented by the provider as part of the service: It MUST be ensured that no default passwords are applied to the system.

If hardware is to be implemented by the provider as part of the service: It MUST be ensured that all updates and patches available at the time of installation have been installed.

If hardware is to be implemented by the provider as part of the service: It MUST be ensured that only those services are activated / installed that are absolutely necessary for the agreed scope of functions.

6. Endpoint device security

Endpoint device refers to an internet-connected computer hardware device on a TCP/IP network (e.g., desktop computers, laptops, smart phones, printers, etc.)

6.1 Delivery

It MUST be ensured throughout the packaging and transport route, that all equipment is adequately protected against damage and manipulation.

There SHOULD be a standardized process for recording, processing and closing out faulty deliveries.

6.2 Handling of client information

It MUST be ensured via end-to-end identity and access management, that only those employees have access to BASF data (incl. order data) who actually need it for their work (need-to-know).

It MUST be ensured, that all subcontractors involved in BASF orders must sign a non-disclosure agreement (NDA) before commencing the order.

6.3 Product Security

There SHOULD be a process in existence to ensure the functionality of distributed endpoint devices (internally by the supplier or upstream by the manufacturer).

If endpoint devices are to be implemented by the provider as part of the service: It MUST be ensured that no default passwords are applied to the system.

If endpoint devices are to be implemented by the provider as part of the service: It MUST be ensured that all updates and patches available at the time of installation have been installed.

If endpoint devices are to be implemented by the provider as part of the service: It MUST be ensured that only those services are activated / installed that are absolutely necessary for the agreed scope of functions.

7. Network Component Security

A network is a collection of computers, servers, mainframes, peripherals, or other devices connected to allow data sharing.

Network components are physical devices required for communication and interaction between devices in a computer network. In particular, they mediate data in a computer network, e.g. cables, plugs, router, switches etc.

7.1 Resource Management

There MUST be an internal resource management system in place to ensure that all projects are adequately staffed with qualified personnel.

7.2 Delivery

It MUST be ensured that the packaging and transport route of all equipment is thoroughly and adequately protected against damage and manipulation.

There SHOULD be a standardized process for recording, processing and closing out faulty deliveries.

7.3 Handling of client information

It MUST be ensured via end-to-end identity and access management, that only those employees have access to BASF data (incl. order data) who actually need it for their work (need-to-know).

It MUST be ensured, that all subcontractors involved in BASF orders must sign a non-disclosure agreement (NDA) before commencing the order.

7.4 IT-Administration

It MUST be ensured that no default passwords are applied to the system.

It MUST be ensured that all updates and patches available at the time of installation have been installed.

It MUST be ensured that only those services are activated / installed that are absolutely necessary for the agreed scope of functions.

7.5 Vulnerability Management

There MUST be a process in place to install security critical updates immediately.

There MUST be a process in place to ensure that all changes are tested on dedicated test systems before they are put into production.

There SHOULD be a process in place to ensure that all known components are regularly scanned for known vulnerabilities.

7.6 Identity and access management

It MUST be ensured via end-to-end identity and access management, that only those employees have access to BASF data (incl. order data) who actually need it for their work (need-to-know).

It SHOULD be ensured via end-to-end identity and access management that employees only have the necessary authorizations (least privileged).

There MUST be a defined process in place to ensure that personnel changes are reflected in the assigned roles and permissions (Joiner-Mover-Leaver).

7.7 Physical Security

Rooms in which hardware components are stored SHOULD be lockable.

External persons SHOULD be accompanied by employees while they are on the company premises.

8. Software/Application Security

Software is a set of instructions, data or programs used to operate computers and execute specific tasks. An application is a computer software package that performs a specific function.

The Software and Applications section includes all software products that are installed locally on servers or clients so that no data is transmitted to third parties.

If software solutions are operated on external systems, the catalog for cloud security should be queried.

8.1 Security Concept

An up-tp-date IT security concept MUST exist for the application.

The current IT security concept MUST be made available to BASF on a regular basis

8.2 IT Service Desk

There MUST be an IT service desk available during normal business hours.

There SHOULD be an IT service desk that can be reached outside normal business hours.

8.3 Data encryption

Standardized cryptographic procedures MUST be implemented and documented to ensure the confidentiality, integrity and authenticity of the transmitted data.

All connections MUST be encrypted as a matter of principle.

8.4 Identity and access management

Rights for the application MUST be managed via a central IAM at BASF, such as active directory.

8.5 Software security

Updates MUST be provided via encrypted channels.

If external libraries are used only as secure classified libraries MUST be used.

Hash values SHOULD be provided for all packages to verify the integrity of downloads.

9. Cloud Security

A cloud service is the provision of a cloud-based platform, management of private clouds or offering of on-demand cloud computing components, e.g. IaaS, PaaS, SaaS.

9.1 Security Concept

An up-to-date IT security concept MUST exist for the application.

The current IT security concept MUST be made available to BASF on a regular basis.

9.2 IT Service Desk

There MUST be an IT service desk that is available during normal business hours.

There SHOULD be an IT service desk that can be reached outside normal business hours.

9.3 Handling of client information

There MUST be a standard process in place to ensure the confidentiality of client information at all times before, during and after projects.

Critical protection requirement: It MUST be ensured, that confidential documents are not left unattended in unlocked offices.

9.4 Information validation

In the case of particularly critical tasks, it SHOULD be ensured that these are always carried out via the dual control principle (e.g. preparation of final reports).

It MUST be ensured that all information used in the course of the project is adequately validated by a standardized process.

9.5 Data encryption

Standardized cryptographic procedures MUST be implemented and documented that ensure the confidentiality, integrity and authenticity of the transmitted data.

Critical protection requirement: Data transfers MUST be classified into different data classification level.

All connections MUST be encrypted as a matter of principle.

9.6 Identity and access management

It MUST be ensured via end-to-end identity and access management that only those employees have access to BASF data who actually neet it for work on a given project.

It SHOULD be ensured via end-to-end identity and access management, that employees only have the necessary authorizations (least privilege).

There MUST be a defined process in place to ensure that personnel changes are reflected in the assigned roles and permissions (Joiner-Mover-Leaver process).

9.7 Software security

IT management MUST ensure that only current software versions that are permissible in terms of cyber security best practices are used to process BASF data.

There SHOULD be a test environment in which software changes are tested previously to productive use.

There SHOULD be a process in place to ensure that all updates and patches are obtained from secure sources only.

There MUST be a process in place to ensure that security-critical updates in particular are installed promptly.

9.8 Backups

Regular information back-ups MUST be performed.

9.9 Malware protection

There MUST be a policy in place to prevent malware.

Critical protection requirement: The use of removable media MUST be restricted.

9.10 Physical Security

Rooms in which endpoint devices are stored SHOULD be lockable.

External persons SHOULD be accompanied by employees while they are on the company premises.

9.11 Compliance

There MUST be a process in place to ensure that all applicable compliance requirements are met before, during and after a project.

9.12 Data Privacy

A data protection officer SHOULD be appointed.

The organization SHOULD have a comprehensive privacy management system.