Annex

IT and Non-IT Cyber Security Provisions for the US

Version 1.0

Date: 13th May 2026

The following CS provisions CS1 through CS15 apply to Contractor and all Contractor Personnel:

CS1 Contact Persons. Contractor must designate one or more contact persons for core cyber security roles and must provide contact information for such individuals to BASF. At least one contact person must respond to all written inquiries from BASF on cyber security issues (such as regarding implemented security measures or potential cyber security incidents) within a reasonable period of time not to exceed 72 hours. If Contractor discovers one or more cyber security incidents affecting Contractor where the incident directly impacts the confidentiality, integrity or availability of BASF information, then Contractor must inform BASF by email to: third-party-breaches@basf.com as soon as possible (not to exceed 72 hours).

CS2 Cyber Training. All Contractor Personnel must receive regular (at least once per calendar year) awareness training on cyber security topics that could impact Contractor's or BASF's systems, products or services.

CS3 Security Procedures. Contractor must comply with all BASF rules, regulations and policies regarding systems and data security procedures (including but not limited to those relating to remote access and those set forth in these Cyber Security Provisions) provided to Contractor and must maintain reasonable technological and organizational measures for the protection of all data including but not limited to Confidential Information.

CS4 ISMS. Contractor must have an information security management system (ISMS) sufficient to identify and manage cyber security risks as appropriate to the type and sensitivity of the data and Confidential Information available pursuant to provision of the Services and must fully implement and maintain such ISMS. Such ISMS must include (but is not limited to):

(1) a process for handling cyber security incidents

(2) limited access to BASF information only to those having a need-to-know such information to provide the Services

(3) use malware protection solutions to mitigate the risk that malware is installed on any devices and servers housing or having access to BASF information

(4) suitable segmentation of Contractor network based on criticality regarding confidentiality and availability requirements of processed data

(5) regularly conducted scans (either by Contractor or a third party) of Contractor's systems and solutions for vulnerabilities, which scans result in either patching or mitigating the identified vulnerabilities using Commercially Reasonable Efforts and time frame (unless such vulnerabilities are related to security of BASF information, in which case vulnerabilities must be patched or mitigated as soon as possible)

(6) a process for immediate installation of security-relevant updates and patches of all software solutions in use

(7) regular exercises in data backup and recovery

(8) separate development, testing and operational environments

(9) secure coding specifications for each programming language and appropriate training to developers using such languages

(10) secure baseline builds, configurations or the like to harden and manage all endpoints such as servers, laptops, and mobile devices and

(11) use of cryptography for protecting the confidentiality, integrity and/or authenticity of BASF data.

Contractor may evidence compliance with the above by achieving current certification under an industry standard framework (e.g., ISO 27001; NIST; NIS 2).

CS5 Encryption. Contractor must encrypt the data and Confidential Information available to Contractor under the Contract using encryption methodologies and techniques which are appropriate to the type and sensitivity of such information on all Contractor devices, data transfer systems and storage locations. Contractor must have the ability to remotely wipe or remove BASF data from any mobile devices.

CS6 Backups. Contractor must apply regular backups to all locations and devices where or on which BASF data and data relevant to the Services is stored.

CS7 Physical Security. Contractor must use physical security measures (such as, but not limited to, locked server rooms and offices and escorted visitor policies) at all locations where BASF data and data relevant to the Services is stored or available.

CS8 Contractor Security Mechanisms. Contractor must implement security mechanisms within Contractor's system and provide documentation of same to BASF if requested. Such systems must encrypt data during storage and in transit.

CS9 Multifactor Authentication. If Contractor is supplying a system solution, then Contractor must either (1) implement multifactor authentication upon set-up or delivery or (2) provide BASF the ability to implement such multifactor authentication in order to access sensitive data on the solution and for configuration changes. Such solution must have functionality allowing granular roles and permissions to be granted to manage such roles and permissions as a configuration change. For any system solution to which Contractor has continuing access,

Contractor must review all roles and permissions on at least an annual basis and, upon written request, provide evidence of same to BASF.

CS10 Updates. Contractor must provide or make available updates and patches as soon as possible after release and must promptly communicate such updates to BASF for installation.

CS11 Testing. The solution must: (1) allow BASF to conduct penetration testing on the solution on regular and as-needed bases either by BASF itself or via a third-party at BASF's expense or (2) Contractor must provide proof that a penetration test was completed by a neutral third-party.

CS12 Instructions. Contractor must deliver to BASF (with or prior to delivery of Services) user instructions that enable user groups to use the solution(s) provided by Contractor in the intended manner for the intended purpose. User instructions must include but are not limited to detailed explanations of security controls.

CS13 Administrator Instructions. Contractor must deliver to BASF (with or prior to delivery of the solution) administrator instructions that enable administrators responsible for operating the solution to manage the solution as intended. Administrator instructions must include but are not limited to detailed explanations of security controls that are available to administrators.

CS14 Design Architecture. Contractor must design both the architecture and the processes for data processing within any solution provided by Contractor to protect such solution and the processed data from unauthorized access and to ensure that no other BASF systems can be accessed if individual components of such solution are compromised. Contractor must provide to BASF upon request documentation of compliance with this section.

CS15 Vulnerabilities. Contractor must use Commercially Reasonable Efforts to mitigate the risk that any solution or any components of a solution contain vulnerabilities that could be manipulated or used to access or compromise the BASF infrastructure or information.

*In addition to the above provisions, the **Section CS16** and **Section CS17** apply if (but only if) Contractor is providing solutions that are operated on Contractor's infrastructure or by an upstream vendor and such solutions require internet access to function (each a "**Cloud Solution**") such as but not limited to Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS):*

CS16 Secure Data Center. Contractor must ensure or receive contractual assurances from the host of the Cloud Solution that all Cloud Solutions are operated in a secure data center protected from physical access by unauthorized third parties.

CS17 Cloud Solution Requirements. If the Cloud Solution is self-hosted by Contractor, then Contractor must meet the following physical protection requirements:

(1) Fire extinguishing and prevention system

(2) Multiple fire compartments as appropriate

(3) Hazard alarm system

(4) Video surveillance system

(5) Automated monitoring of the infrastructure

(6) Connection of the data center to a central, 24/7 manned control station

(7) Temperature and humidity management

(8) Uninterruptible power supply and

(9) Surge protection device

CS18 If (but only if) Contractor is providing information technology hardware to BASF, then the following apply:

(a) Contractor must ensure that all such hardware components are protected from unauthorized access or control and proactive measures are implemented to mitigate the risk that hardware components could be manipulated or used to access or compromise BASF infrastructure or information.

(b) Contractor must deliver all hardware components fully functional and in the intended configuration for use.

(c) Contractor must test all hardware components in terms of functionality and integrity by Contractor or its upstream vendor. Contractor must ensure that sufficient technical documentation is available for all hardware components to enable BASF to select the optimal components for a given application.

(d) Contractor must ensure that all security-relevant updates and patches available at the time of installation are installed on all devices and that all initial passwords are configured so that they must be changed by the user at the first login.