Planon
Building Connections

PLANON CYBER SECURITY

v24.04

Version: v24.04

Date: 17 april 2024

Author: Information Security & Data Protection Office

Document data
History

Name	Date	Version	Status	Description
PLANON CYBER SECURITY	25 November 2023	V23.01	Draft	
PLANON CYBER SECURITY	27 February 2024	V24.01	Draft	Discussed with legal team
PLANON CYBER SECURITY	17 April 2024	V24.04	Final	Legal / ISDPO Team

Distribution-list

Name	Date	Version	Department
PLANON CYBER SECURITY	25 January 2023	V23.01	Information Security & Data Protection Office

PLANON CYBER SECURITY REQUIREMENTS

The following Cyber Security and Information Security requirements, as outlined by Planon (hereinafter referred to as "**Cyber Security Requirements**"), apply to all potential and existing SupplierSuppliers, suppliers, or any other entities involved in supplying digital information systems and/or other services to Planon (collectively referred to as "**Suppliers**" and individually referred to as "**Supplier**") as defined in various agreements such as General Purchase Terms & Conditions, Software License Purchase Agreement or any other purchase-related agreement with Planon (collectively referred to as "**Agreements**" and individually referred to as "**Agreement**").

Each Agreement governs the contractual relationship between Planon Shared Services B.V. or any of its affiliated companies (collectively referred to as "**Planon**") and the Supplier and are subject to the specific terms of the order for products, supplies, software, and/or services (collectively referred to as "**Supply**") as outlined in the specific purchase order, project specification, or any other document governed by such Agreement (hereinafter referred to as "**Order**"). For the avoidance of doubt, the Supply is only for internal Planon use. These terms exclude any other terms that the Supplier seeks to impose or incorporate. For the purposes hereof, Planon and the Supplier are collectively referred to as the "**Parties**" and individually as a "**Party**".

The Supplier acknowledges that compliance with these Cyber Security Requirements is critical for Planon when procuring the Supply from the Supplier. The obligations for the Supplier, as set forth in these Cyber Security Requirements, constitute essential obligations of the Supplier in providing the Supply to Planon. These obligations also apply to any subcontractors of the Supplier and their subcontractors.

1 DEFINITIONS

1.1 "**Planon Data**" means all data and knowledge in various formats, including paper, digital and electronic, owned by Planon. This includes data and information in any form obtained, received or accessed by the Supplier from Planon or its affiliates or subcontractors of the Supplier and their subcontractors, including the creation, generation, processing, transmission, storage or management on behalf of Planon or its Suppliers. Furthermore, "Planon Data" includes also any personal data.

1.2 "**Digital Assets**" means a) information technology systems, operational technology systems and information and communication networks, b) internet-enabled applications and devices, c) applications, devices, and terminals for accessing, seeing, reading, using, processing, transmitting, transferring, storing, treating and/or handling data, including Planon Data, and d) the data, including Planon Data, contained within such systems and networks.

1.3 "**Cyber Security Event**" means a single or a series of unwanted or unexpected events affecting the confidentiality, integrity and/or availability of information that have a significant probability of compromising business operations and threatening information security.

1.4 "**Cyber Security" means the protection to defend internet-connected devices and services from any malicious attack(s).**

2 CYBER SECURITY PRINCIPLES

2.1 **Information Security Management System (ISMS).** The Supplier is responsible for implementing and sustaining effective security systems, technologies, methods, protocols, policies, strategies, and safeguards. This includes conducting all necessary activities and employing all reasonable efforts to develop, uphold, and progressively enhance its information security measures, specifically concerning Planon Data.

2.2 **Cyber security procedures and Information Security Protocols.** The Supplier must implement, uphold, and enforce all relevant strategies and protocols, undertake all necessary actions, and apply all suitable measures aimed at ensuring effective and efficient response, prevention, mitigation, and recovery from a) any Cyber Security Events and its consequences, and b) any potential Cyber Security Event and its possible impacts, particularly concerning Planon Data.

2.3 **Data storage and Secure Data Handling**. The Supplier is required to guarantee that the data storage facilities and any other locations under their control where Planon Data is stored or processed are safeguarded using robust and suitable security measures and practices. The Supplier must adopt and adhere to globally acknowledged best practices for data storage facilities and any other locations where Planon Information is stored or processed.

2.4 **Representative compliance**. The Supplier must take all necessary actions to ensure that its third party agents involved in the tasks, services or activities under the Agreement and Order comply with all provisions and obligations specified in these Cyber Security Requirements.

2.5 **Third party services**. The Supplier must implement all necessary measures to guarantee that any external party offering services on behalf of the Provider, in connection with any contract between the parties, adheres to all conditions and obligations outlined in these Cyber Security Requirements.

3 MANAGEMENT, EMPLOYEES, SUBCONTRACTORS and SUPPLIERS

3.1 **Information security management system. Documentation of Security Management Practices**. The Supplier is required to maintain and enforce a suitably documented system for managing information security ("**Information Security Management System**" or "**ISMS**"). This ISMS must encompass and adhere to all the criteria of an internationally recognized standard in cyber security. Its effectiveness should be regularly validated through internal and/or independent external evaluations conducted by certified professionals. The ISMS must establish clear cyber security goals, including a formal cyber security policy, ensuring these goals are in sync with the Supplier's organizational aims and the stipulations of these Cyber Security Requirements.

3.2 **Security Awareness and Education Initiatives**. The Supplier must implement a suitable program for raising awareness and training in Cyber Security, delivering informational sessions and training regularly. The primary goals of this initiative are to consistently foster and enhance the understanding of cyber security among employees and any third parties involved in cyber security services, as well as to cultivate a proactive stance towards Cyber Security.

3.3 **Third party Risk.** The Supplier is responsible for implementing a suitable risk-focused approach for choosing and overseeing its subcontractors and Suppliers. It's the Supplier's responsibility to guarantee that provisions related to Cyber Security are included in contracts with these subcontractors and/or Suppliers. Furthermore, the Supplier must ensure these stipulations are fulfilled and consistently reviewed on an annual basis and at any other pertinent times.

4 ASSET MANAGEMENT

4.1 **Asset Management.** The Supplier is required to uphold and enforce relevant policies and protocols for the identification, categorization, and oversight of used assets in its services throughout their lifecycle, from acquisition to disposal.

4.2 **Record of Assets**. The Supplier must keep an up-to-date record of assets, reflecting the current status of their information and communication systems, and identifying key applications and infrastructure components, inclusive of cloud services where applicable. This inventory should be regularly updated and reviewed, especially when assets are added, removed, or modified.

4.3 **Authorised Assets**. The Supplier must ensure that all technology equipment authorized for storing or handling Planon Data is properly recorded in a designated record of assets and meets the following criteria at all times:

- Designated ownership with individuals accountable for the security of the devices during their lifespan.
- Continuous monitoring for compliance with established standards.
- Automatic updates of anti-malware software.
- Regular application of patches and updates issued by the Supplier's IT department.
- Scheduled weekly intervals for potential emergency updates.
- Configuration to block updates from sources not approved by the Supplier's IT team or a verified anti-malware provider.

4.4 **Network Assets.** The Supplier must ensure that assets involved in storing, transmitting, or processing Planon Data and connected to the internet are secured with adequate network safeguards and Cyber Security measures, such as firewalls or network segmentation.

5 BUSINESS RESILIENCE

5.1 **Business Continuity**. The Supplier is responsible for establishing, maintaining and implementing documented and periodically reviewed operational continuity policies and processes.

5.2 **Identification of Essential Systems**. It is the Supplier's responsibility to identify and record systems critical to operations.

5.3 **Cyber Security Event procedures**. The Supplier must develop and maintain appropriate policies and processes to ensure operational resilience in the event of a Cyber Security IEvent.

5.4 **Business Continuity Plan**. The Supplier is obliged to develop and maintain a relevant operational continuity strategy. This strategy must be activated in the event of disruptions to the services provided to Planon.

5.5 **Back-ups and Recovery**. The Supplier is required to establish and maintain automated data backup systems. The Supplier must have systems and protocols in place for alert notifications in case of backup failures. In addition, the Supplier must ensure regular testing of data backup processes to confirm data recovery capabilities in scenarios such as data corruption or cyber security events.

6 CYBER SECURITY EVENTS

6.1 **Notification of Cyber Security Events.** In the event the Supplier becomes aware of a Cyber Security Event that affects, or poses a risk to, the security of the Supplier or the Planon Data, the Supplier must immediately notify Planon's Security Team, no later than twenty-four 24) hours after becoming aware of such event, via email at soc@planonsoftware.com. This notification must include a description of the Cyber Security Event and the Supplier's primary contact person.

6.2 **Response to Cyber Security Events.** If a Cyber Security Event affects either the Supplier or Planon, the Supplier is obliged to:

(a) Promptly take all necessary measures, actions and procedures, to contain tor limit the Cyber Security Event.

(b) Promptly provide Planon with written details of how the Supplier intends to continue to comply with its obligations under these Cyber Security Requirementsto mitigate and address the Cyber Security Event and its impact on Planon's digital systems, including Planon Data. Planon expects the Supplier to provide information on, but not limited to:

i) The nature of the Cyber Security Event.

ii) The date and time when the Cyber Security Event occurred.

iii) Planon Data which are or may be affected by the Cyber Security Event.

iv) Any measures to be taken, performed and proposed to avoid, limit, and overcome the Cyber Security Event and its effects within and in relation to the provided services towards Planon, including Planon's Data.

v) The Supplier must share all information with Planon that may assist in taking measures and carrying out activities to prevent, mitigate and address the Cybersecurity Event and its impact on Planon's digital systems, including the Planon Data.

(c) The Supplier must, at its own expense, promptly:

i) Supply Planon with all necessary information related to any Cyber Security Event and its impacts on Planon's digital systems, including Planon Data, as well as any actions taken or proposed to address these issues.

ii) Implement all necessary measures and conduct all appropriate activities, including those required by Planon, to prevent, mitigate, and address any Cyber Security Event and its impacts on Planon's digital systems, including Planon Data.

iii) Cooperate with Planon in any suitable way to support Planon in taking measures and performing activities to prevent, mitigate, and address any Cyber Security Event and its impacts on Planon's digital systems, including Planon Data.

iv) Compensate Planon for all costs, expenses, and losses incurred or suffered due to the Cyber Security Event and its impacts on Planon's digital systems, including Planon Data.

7 INDEMNITY

7.1 Supplier will indemnify, keep indemnified and hold Planon harmless in full and on demand from and against all liabilities, direct, in direct and consequential losses, damages, claims, proceedings and legal costs (on an indemnity basis), judgments and costs (including costs of enforcement) and expenses which Planon incur or suffer directly or indirectly in any way whatsoever as a result of or in connection with a breach of, or a failure to perform, or a delay in performance or negligent performance of, any of Supplier's obligations under these Cyber Security Requirements, the Agreement and/or the Order.

8 INSPECTATION AND AUDIT

8.1 Upon Planon's request, Supplier shall provide all evidence required by Planon to conduct a thorough investigation within the scope of the provided services for compliance with the agreed Cyber Security Requirements. Planon reserves the right, directly or through a representative duly authorized by Planon, to conduct any inspection of Supplier and/or the deliverables, including on the premises of Supplieror its major subcontractors (where feasible possible), provided that Planon gives reasonable advance notice and conducts the inspection during normal business hours of Supplier/those subcontractors (or at any time in case of emergency), in order to:

(a) examine Supplier's Information Security Management System;

(b) inspect, in any manner, the works and/or services making up the Supply, in the process of being made;

(c) inspect, in any manner, the quality, manufacturing and test data for the Supply; and

(d) inspect, in any manner, Supplier's actual compliance with its undertakings and/or obligations under the Order and/or these Cyber Security Requirements.

In the event that the audit outcome revailt that Supplier is not compliant with the undertakings and/or obligations under the Cyber Security Requirements, then all cost for the audit as well as, if applicable, all costs related the the remedy of such non-compliance are for Supplier.

9 TERMINATION

9.1 If Supplier fails to fulfil any of its undertakings and/or obligations under the Cyber Security Requirements, Planon may terminate the Agreement and/or Order without any need for any other formality, fifteen (15) calendar days after formal notice, provided that following such termination:

(a) any article(s) which expressly or impliedly continue to have effect after expiry or termination will continue in force;

(b) all other rights and obligations will immediately cease without prejudice to any rights, obligations, claims (including claims for damages for breach), liabilities and/or indemnities which have accrued prior to the date of expiry of termination.

10 INSURANCE

10.1 At Planon's request, and in any case within ten (10) days from Order acceptance, Supplier shall provide all certificate(s) of insurance to be issued by its insurers, covering to a reasonable extent the risks associated with the fulfilment of the Order and, in all cases for a minimum insured amount of five million Euro (€5.000.000) and to obtain, at is own expense, any reasonable additional cover that Planon deems necessary based on the risks associated with the fulfilment of the Order.