Basic Information Security Requirements for business partners

The following information security requirements apply to all business partners (hereinafter referred to as "business partners") of Securitas.

1. The business partner must implement appropriate organisational and technical measures to ensure the confidentiality, authenticity, integrity and availability of the business partner's operations, as well as its products and services. These measures must comply with good industry practice and include an appropriate information security management system that complies with standards such as ISO/IEC 27001 or the BSI Basic Protection Scheme, and must include at least the following for staff:
   i. General security awareness training;
   ii. Authentication requirements for employees;
   iii. Access authorisations that comply with the principles of 'least privilege' and, where applicable, 'segregation of duties';
   iv. Endpoint cybersecurity measures, which may include antivirus protection, application controls or other appropriate systems;
   v. Audit logging of systems that access, store or process the business partner's critical data;
   vi. Backup, recovery and business continuity measures to ensure the continuity of business operations (e.g. during a ransomware incident).

   The term 'business partner's operations' refers to all assets, processes and systems (including information systems), data (including data belonging to Securitas and its customers), personnel and locations that the business partner uses or processes from time to time in the performance of this contract.

2. Should products or services contain software, firmware, chipsets or integrated circuits, the following shall apply:
   i. The Business Partner must adhere to secure, state-of-the-art software development methods, including secure coding standards, e.g. OWASP standards;
   ii. the Business Partner shall implement appropriate standards, procedures and methods to prevent, identify, assess and remedy vulnerabilities, malicious code and security incidents in products and services, in line with industry best practices and standards such as ISO/IEC 27001 or BSI Basic Protection;
   iii. the business partner shall furthermore provide support and services for the repair, updating, upgrading and maintenance of the products and services, including the provision of patches to Securitas to remedy vulnerabilities throughout the reasonable lifespan of the products and services;
   iv. the business partner grants Securitas the right to test the products or software components supplied by it for malicious code and vulnerabilities at any time and shall provide Securitas with appropriate support in this regard;
   v. the Business Partner shall provide Securitas with a point of contact for all matters relating to information security (available during business hours).
   vi. Where artificial intelligence is used, Securitas data must not be used for training the AI.

3. The business partner is obliged to report immediately and without delay to the Securitas contact person named to them and to the following Securitas information security contact addresses all relevant information security incidents that have occurred or are suspected to have occurred, as well as any vulnerabilities discovered in the business partner's operational processes, services and products of the business partner, if and to the extent that Securitas is or could be significantly affected by them:
   i. for security incidents and security vulnerabilities ('Vulnerabilities'): informationssicherheit@securitas.de

4. The business partner shall take appropriate measures to ensure that its subcontractors and suppliers undertake similar obligations, as required by these information security requirements, within a reasonable period of time.
5. Where 'Securitas data' is processed and stored, it must be GDPR-compliant – EU location.
6. For privileged access to Securitas systems or applications, the roles and responsibilities for privileged access management of provider administrators (identity management, granting access, revoking access, access auditing) must be applied, and the business partner must comply with the Acceptable Use Policy for privileged accounts.
7. The business partner has implemented a failover plan, backups and DRM/BCM relating to the service provided to Securitas.
8. There is cyber insurance or a relevant incident response plan in place to cover losses resulting from security breaches on the part of the business partner.
9. Only secure protocols may be used when connecting to Securitas systems.
10. The business partner is obliged to provide Securitas, upon request, with written evidence of compliance with the information security requirements, including generally recognised audit reports (e.g. ISO 27001, SoA and Scope documents).
11. Securitas is entitled to verify the business partner's compliance with the provisions of these information security requirements at the business partner's premises, subject to reasonable notice, if Securitas has reasonable grounds to suspect that the business partner is not complying with them.