Henkel Cybersecurity Requirements

Cybersecurity measures

Supplier shall implement and continuously improve adequate technical and organizational measures following commonly accepted standards to **manage the security of information and IT services and to defend against cybersecurity incidents** (e.g., ISO 27001). Those measures shall satisfy the applicable requirements (depending on the services/products provided) and comprise the following areas *(corresponding ISO 27002:2022 reference in brackets)*:

1. Supplier shall define and maintain a set of policies for information security. *(5.1)*
2. Supplier shall define roles and responsibilities for IT security and assign suitable staff. *(5.2)*
3. Supplier shall keep Henkel information confidential, use it only to the extent required to fulfill the agreed services and have respective organizational measures in place (including e.g. confidentiality agreements with staff and business partners; documented procedures for handling customer data). *(6.6)*
4. Supplier shall conduct reasonable background verification on employment candidates in accordance with job role requirements, relevant laws, regulations, and ethics. *(6.1)*
5. Supplier's contracts with employees and contractors shall state their responsibilities for security. *(6.2)*
6. Supplier's management shall ensure that employees and contractors are aware of and fulfil their information security responsibilities and shall conduct regular security training for employees. *(6.3)*
7. Supplier shall identify all organizational assets required for the services and apply adequate protection measures proportionate to their risk. *(5.9)*
8. Supplier shall define, document, and implement adequate access controls based on business and security requirements to prevent unauthorized access to Henkel data; these shall follow the need-to-know principle and include joiner-mover-leaver processes and periodic access reviews. *(5.15)*
9. Supplier shall implement multi-factor authentication and single sign-on for key IT systems. *(8.5, 8.2)*
10. Supplier shall implement Privileged Access Management (PAM) technologies to enforce secure handling of privileged credentials, controlled elevation of privileges, and monitoring of privileged access to key IT infrastructure and IT applications. *(8.2)*
11. Supplier shall implement suitable controls for the protection of non-human identities (such as service accounts or API keys), including limiting authentication to allow-listed IP ranges, automated processes for provisioning/de-provisioning, secret/key rotation, and secure storage of secrets in vaults. *(5.16)*
12. Supplier shall ensure that cloud services used exclusively for Henkel are not publicly accessible (e.g. by restricting access to allow-listed Henkel IP ranges). *(8.22)*
13. Supplier shall ensure that Henkel's data is securely segregated from other customers' data. *(8.20)*

14. Supplier shall prevent unauthorized physical access to, and damage of, information and information processing facilities, (e.g. by site access restrictions, visitor management, protection against relevant environmental threats). *(7)*
15. Supplier shall protect information and information processing facilities against malware with industry standard detection and response measures, including Endpoint Detection and Response (EDR) solutions. *(8.7)*
16. Supplier shall log security events, protect them against tampering, and analyze them to enable timely detection of security incidents. *(8.15)*
17. Supplier shall monitor networks, systems and applications for anomalous behavior, including cyberattacks, with industry-standard measures and respond promptly to potential or confirmed security incidents. *(8.16)*
18. Supplier shall protect networks through appropriate security controls (e.g. traffic filtering, intrusion detection and prevention, network segmentation, web application protection, and protection against Distributed Denial of Service (DDoS) attacks). *(8.20 – 8.22)*
19. Supplier shall establish incident response capabilities to ensure an immediate and effective response to information security incidents. *(5.24 – 5.28)*
20. Supplier shall report security incidents which may affect Henkel to infosec@henkel.com without undue delay and ideally within 1 hour in accordance with legal reporting requirements. *(5.24)*
21. Supplier shall manage technical vulnerabilities through hardening, regular identification (e.g. by scans), risk assessment, and timely remediation. For cloud environments, Supplier shall continuously monitor for and remediate security misconfigurations using appropriate cloud posture management solutions. *(8.8)*
22. Supplier shall protect information in transit and at rest when available and using industry-standard cryptography. Cryptographic keys and certificates shall be securely stored, e.g. in dedicated key-management systems or secure vault solutions. *(8.24)*
23. If Supplier develops information systems, Supplier shall integrate adequate information security measures throughout the system and software development lifecycle. This includes secure coding practices, automated security testing (e.g., SAST for proprietary code, SCA for libraries, DAST for deployed applications), testing of security functionality, and regular penetration testing. *(8.25 – 8.29)*
24. Supplier shall ensure separation of operational from non-operational IT environments to prevent unauthorized access, unintended changes, and cross-environment interference. *(8.31)*
25. Supplier shall maintain and operate a documented change management process to ensure that all changes to information processing facilities and information systems are properly authorized, tested for security and functionality, formally approved, and implemented in a controlled manner. This process shall include the handling of emergency changes. The Supplier shall maintain retrievable documentation of all changes, including test results and approvals. *(8.32)*
26. Supplier shall maintain a capacity management process to ensure system resources are continuously monitored, analyzed, and adjusted to meet agreed service levels. *(8.6)*

27. Supplier shall implement and maintain backup processes, including the use of immutable backups for critical systems and regular restoration tests to verify backup effectiveness. *(8.13)*
28. Supplier shall operate organizational and technical measures, including a documented business continuity management (BCM) plan, which is regularly updated and tested to ensure the agreed service availability levels are maintained. *(5.29)*
29. Supplier shall regularly review its technical and organizational measures (e.g. management reviews, performance metrics, and continuous improvement activities) to ensure that information security is implemented and operated effectively. *(5.35 – 5.36)*
30. Supplier shall ensure that breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements are avoided. *(5.31)*
31. Supplier shall only outsource IT services to, or share Henkel information with, third parties that are bound by written contract to information security requirements. Those information security requirements must not be less protective than the requirements in this document. *(5.20)*
32. Supplier shall regularly monitor, review, and audit the security of IT services they have outsourced (e.g., IT hosting, cloud services). *(5.22)*

Audit rights and independent audit report

Supplier shall grant Henkel the **right to audit and to monitor** the service provision. Audits may be conducted once per year during normal business hours, upon reasonable advance notice. Supplier shall provide Henkel with respective information and reasonable assistance to carry out such audit. The scope of such audit will be agreed upon with the Supplier, the scope will be only related to the contracted service, not affecting supplier's business secrets and supplier's other customers' data. Monitoring is a continuous operational activity to verify the delivery of contracted services. It may include the responsible identification and reporting of security vulnerabilities, carried out in a non-disruptive and non-damaging manner and strictly limited to the contractually agreed scope of online services.

Depending on the contracted services, the supplier provides Henkel with **independent external audit reports or certificates** covering the services, e.g., ISO 27001 or TISAX certificates, SOC 2 Type 2 or ISAE 3402 Type II reports for services relevant to financial accounting. If the services include the **hosting** of Henkel information on central systems (e.g., software-as-a-service, infrastructure-as-a-service, IT hosting), Supplier shall provide, on an annual basis, a SOC 2 Type 2 report and a penetration test report.

The Supplier acknowledges by signature the above Cyber Security Requirements.

Supplier's legal entity information and signature

Post address incl. country:	Click or tap here to enter text.
Name and position of signee:	Click or tap here to enter text.
Location and date of signature:	Click or tap here to enter text.
Signature:	Click or tap here to enter text.