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 (e.g. confidentiality agreements with staff and business partners) *(6.6)*
4. Supplier carries out 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. *(6.3)*
7. Supplier shall identify all organizational assets required for the services and protect them adequately. *(5.9)*
8. Supplier shall define, document, and implement adequate access control concepts based on business and security requirements following the need-to-know principle to prevent unauthorized access to Henkel data. *(5.15)*
9. Supplier shall implement multi-factor authentication, single-sign-on and privileged access management technologies for their key IT systems. *(8.5, 8.2)*
10. Supplier shall implement suitable controls for the protection of non-human identities (such as service accounts or API keys) such as limiting authentication to whitelisted IP ranges as well as automated processes for provisioning, secret/key rotation, and de-provisioning *(5.16)*
11. Supplier shall prevent unauthorized physical access, damage, and interference (e.g., environmental threats) to information and information processing facilities required for the services. *(7)*
12. Supplier shall protect information and information processing facilities against malware with industry standard detection and response measures (e.g. an EDR solution on IT endpoints). *(8.7)*
13. Supplier shall log security events, protect them against tampering, and analyze them to timely detect security incidents. *(8.15)*

14. Supplier shall monitor networks, systems and applications for anomalous behavior including cyberattacks with industry standard measures and take appropriate actions to manage potential security incidents *(8.16)*
15. Supplier shall establish management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents. *(5.24 – 5.28)*
16. Supplier shall report security incidents which may affect Henkel to infosec@henkel.com without undue delay in line with legal reporting requirements. *(5.24)*
17. Supplier shall manage technical vulnerabilities, including vulnerability identification (e.g., regular scans, penetration tests), risk assessment, and remediation (including patching, hardening, restrictions of software installations etc.). In Cloud environments supplier shall use a cloud posture management solution to identify and resolve misconfigurations. *(8.8)*
18. Supplier shall manage IT networks to protect information in systems and applications (e.g., through the use of firewalls, intrusion preventions systems, network segmentation). *(8.20 – 8.22)*
19. Supplier shall consider information security requirements right from the beginning when acquiring, developing, or enhancing information systems / software (security by design). *(5.8 and 8.26)*
20. Supplier shall ensure that cryptography is used effectively to protect information. *(8.24)*
21. If Supplier develops information systems, Supplier shall ensure adequate information security measures within the development lifecycle of information systems / software (e.g., change control procedures, secure coding, testing of security functionality, penetration testing). *(8.25 – 8.28)*
22. Supplier shall ensure correct and secure operations of information processing facilities and that operations are documented in operating procedures, including change controls, restricting access to operational software, backups & recovery (including immutable backups for critical systems), IT service continuity, capacity management and separation of operational from other IT environments. *(5.37)*
23. Supplier shall delete Henkel information which is no longer required to fulfill Supplier's services to Henkel. *(8.10)*
24. Supplier shall ensure the continuity and security of the contracted services during adverse situations, e.g., a crisis or disaster, by adequate organizational and technical measures. *(5.29)*
25. 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)*
26. Supplier shall regularly review its technical and organizational measures to ensure that information security is implemented and operated as expected. *(5.35 and 5.36)*.

Audit rights and independent audit report

Supplier shall grant Henkel the **rights to audit and to monitor** the service provision during normal business hours once per year 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.

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 ISAE3402 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 a SOC 2 Type 2 report.

Sub-service providers

Supplier shall only outsource IT services to or share Henkel information with third parties who are bound by **written contract** to information security requirements. Those information security requirements **must not be less protective** than the requirements in this document.

Supplier shall **regularly monitor**, review, and audit the security of IT services they have outsourced (e.g., IT hosting, cloud services).

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.