

IT&D FUNCTIONAL POLICY

Supply Chain Cyber Security Policy

v.1.0 [Final]

Valid from: 20/07/2025

Security Level Public

Next review: 20/01/2027

Policy Owner: IT&D Director - Cyber Strategy & Risk

Do's



Read and comply with all active Policies and Standards appropriate to your area of work and / or the technologies you work with.

Don'ts



Engage in any action or with any Third Party acting in breach of this Policy.

Purpose and Scope

Purpose

The purpose of this policy is to establish a framework for ensuring that third-party entities engaging with Reckitt maintain robust cyber security controls. This policy governs the relationship between Reckitt and its direct suppliers and service providers to mitigate identified cyber security risks which could impact Reckitt.

In implementing this policy, Reckitt seeks to protect its operations, data, reputation, customers, consumers and employees from potential threats posed by third-party vulnerabilities.

Scope

The principles and policy statements described in this policy apply to all third parties engaged with Reckitt, including those organisations contracted to provide goods, services and those in partnerships and joint ventures in any region or location.

This Policy contains generic requirements which apply to all organisations, as well as some additional requirements, e.g. suppliers accessing Reckitt systems, which are applicable only where the third party is engaged in the relevant activity or providing a relevant service or product.

Policy Statement


Policy

The following sections describe the obligations that Reckitt imposes on its contracted suppliers. All suppliers are required to comply with the 'Generic Requirements' section, as well as any additional requirements that are applicable from the subsequent sections.


Generic Requirements

Taking into account the cost of implementation and the potential exposure to Reckitt, all organisations providing goods or services to Reckitt must:

1. Complete and return, on request, cyber security third-party risk assessment questionnaires.
2. Provide Reckitt, on request, access to independent cyber security assessments and penetration tests from a Council of Registered Ethical Security Testing (CREST) approved organisation.
3. Implement and continuously improve an information security governance structure with defined roles and responsibilities, reinforced by information security policies and standards that are communicated to all employees / contractors with disciplinary processes applied if employees commit a security breach.

	Doc Title:	Supply Chain Cyber Security Policy	Version #	1.0
	Doc Ref #:	GLOIT-G7.3-POL130	Effective Date	20/07/2025
	Security Level:	Public	Page 2 of 9	

4. Comply with applicable cyber security regulatory requirements.
5. Conduct background checks on their employees, contractors and third parties.
6. Provide information security awareness training, at least annually to educate their employees and contractors about their security obligations and how to recognize attacks including but not limited to social engineering tactics.
7. Implement protective cyber security controls including but not limited to:
 - Using vendor supported systems with the latest (or at least N-1) security patches installed.
 - Protecting its network(s) using commercially available equipment and industry standard techniques, including firewalls, intrusion detection systems, access control lists and secure routing protocols.
 - Installing and maintaining industry standard (which will comprise the latest version or engine) anti-virus and malware protection software on information systems.
 - Using email security and spam filtering solutions.
 - Enforcing strong authentication and authorization controls including the use of industry standard multifactored authentication for network and information system access.
 - Implementing commercially reasonable physical and electronic security to create and protect passwords.
 - Granting access to information systems rights on a 'least privilege' basis to authorised personnel only.
 - Implementing reasonable physical protection for network and information systems.
 - Monitoring and restricting the use of privileged accounts
8. Identify and manage vulnerabilities that present a risk to the security of network and information systems and have in place a vulnerability management programme to ensure that firmware, operating system, and application software is patched as soon as practicable against critical vulnerabilities.
9. Have a cyber security risk management process which aims to identify and treat cyber security risks.
10. Monitor network and information systems for indicators of compromise
11. Without undue delay, take all steps necessary to mitigate and/or resolve cyber security incidents.
12. Manage cyber security incidents in accordance with pre-defined incident response procedures.
13. Notify Reckitt immediately , of any cyber security incident which:
 - Impacts or may impact on the provision of the products or services to Reckitt, either directly or indirectly.
 - Impacts or may impact on the reputation of Reckitt, its brands, its employees, its customers or its consumers.
 - May lead to a cyber security incident within Reckitt (e.g. through malware

	Doc Title:	Supply Chain Cyber Security Policy	Version #	1.0
	Doc Ref #:	GLOIT-G7.3-POL130	Effective Date	20/07/2025
	Security Level:	Public	Page 3 of 9	

propagation over a network connection or via email).

14. Share with Reckitt any information that subsequently becomes available to it which may assist Reckitt in mitigating and/or preventing any impact of a cyber security incident.
15. Maintain and test disaster recovery, business continuity and incident response policies and procedures, ensuring that the implemented solutions support achievement of contractual service level agreements.
16. Obtain and maintain, at its own costs, cyber security liability insurance with reputable insurers so that the level of cover and other terms of insurance are sufficient to cover the supplier's obligations and liabilities and, in any event, so that each policy provides cover of not less than £5,000,000 (five million pounds) per event or series of events.
17. Cascade the requirements described in this policy to subcontractors involved in the provision of the goods and services to Reckitt.
18. Ensure any critical suppliers and subcontractors are similarly obligated to implement and maintain industry standard cyber security practices.

B. Suppliers processing Reckitt data

The policy statements in this section are applicable to all Reckitt suppliers that process Reckitt data, including confidential, commercially sensitive, or personal information related to Reckitt's business, its employees, customers or consumers.

Suppliers must:

19. Implement appropriate technical and organisational measures (TOMs) to preserve the integrity and keep Reckitt's data secure from loss and unauthorised access, including encrypting data in transit and at rest.
20. Ensure that data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage, and that the target entities for any transfer of data by means of data transmission facilities can be established and verified, with appropriate pseudonymisation and encryption measures adopted to protect the confidentiality of data during transfer and storage.
21. Ensure the establishment of an audit trail to document whether and by whom data have been entered into, modified in, or removed from data processing.
22. Ensure that data are protected against accidental destruction or loss, and appropriate measures adopted to support access to data and / or restoration of data in the event of a physical or technical incident impacting availability.
23. Ensure that data collected for different purposes can be processed separately.
24. Return, securely archive and/or delete Reckitt's data at the end of the contract or agreement term, when the data is no longer required by the supplier in order to provide its goods or services or when instructed to do so by Reckitt.
25. Provide, on request, a Data Destruction Certificate.
26. Notify Reckitt, without undue delay and in any case within 48 hours or within 24 hours for suppliers providing warehousing and/or logistical services, if it suspects or has reason to

	Doc Title:	Supply Chain Cyber Security Policy	Version #	1.0
	Doc Ref #:	GLOIT-G7.3-POL130	Effective Date	20/07/2025
	Security Level:	Public	Page 4 of 9	

believe that Reckitt data has become corrupted, degraded, lost, breached or otherwise affected by or subject to a cyber incident, also providing details of remedial actions the supplier has taken or proposes to take.

27. Comply with all applicable laws and all cyber security requirements in connection with processing of confidential and personal information and shall not by any act or omission cause Reckitt (or any other person) to be in breach of any applicable law.

28. Suppliers must not:

- Use Reckitt's data except for the purpose of exercising or performing its rights and obligations under a signed contract, agreement or statement of work
- Disclose Reckitt's data to any third party except as permitted under a signed agreement or statement of work.

If data is corrupted, lost or sufficiently degraded as a result of the Supplier's default so as to be unusable, Reckitt may:

- require the supplier to restore or procure the restoration of data to the extent possible and supplier will do so as soon as practicable but not later than five (5) days from the date of receipt of Reckitt's notice; and/or
- itself restore or procure the restoration of data and will be repaid by the Supplier any reasonable expenses incurred in doing so.


C.Suppliers Accessing Reckitt's Network & Information Systems

The policy statements in this section are applicable to all suppliers (including their staff and subcontractors) that access Reckitt's network and information systems either in person, via a Reckitt issued and provisioned user account or through a technical process e.g. via an application programming interface (API), Service Account (SA) or bot:

29. Suppliers and their representatives must not use or access any Reckitt network or information system except with Reckitt's prior approval and then only for the sole purpose of providing contracted or agreed services.

30. When accessing any Reckitt system, the supplier must:

- Comply with the same Reckitt cybersecurity requirements that are applicable to Reckitt employees and described in approved and published IT&D policies and standards.
- Not at any time introduce, and shall take all reasonable steps to prevent the introduction of, any programme, routine or device onto any Reckitt network and information systems which is designed to delete, disable, deactivate, interfere with or otherwise cause harm, including but not limited to any virus or vulnerabilities, time bomb, software lock, malicious logic, worm, trojan horse or trap door.
- Ensure that only its authorised employees who have received training as required by Reckitt will access Reckitt's systems, software or hardware, upon request.
- Only use Reckitt's approved solutions to gain system access.

	Doc Title:	Supply Chain Cyber Security Policy	Version #	1.0
	Doc Ref #:	GLOIT-G7.3-POL130	Effective Date	20/07/2025
	Security Level:	Public	Page 5 of 9	

- Ensure that their services are conducted in a manner that prevents and takes all commercially reasonable measures to avoid introducing any faults or malfunctions into Reckitt's networks and information systems.

D. Suppliers of Hardware, Software and Cloud Products

The policy statements in this section are applicable to suppliers that provide network and information system hardware, software (including software-as-a-service applications (SaaS)) and cloud-based products and services.

40. Suppliers must:

- Provide Reckitt, on request, with a Software Bill of Materials for any software that is provided.
- Routinely conduct, or alternatively have an independent CREST approved organisation conduct, vulnerability assessments and provide a copy of such report to Reckitt on request.
- Support Reckitt teams and their preferred partners in running their own independent cyber security assessments of supplied products.
- Routinely determine whether upgrades, patches and fixes, additions or modifications of applicable controls are required and make maintenance releases available to Reckitt without charge.
- Use secure code development standards based on industry best practices.
- Ensure that all code undergoes thorough testing before being included in the Product (also upgrades and patches), including but not limited to peer reviews, Software Composition Analysis (SCA), Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST).
- Remediate any cyber security issues found as a result of the application code review including but not limited to open source and third-party software components.
- Not release updates or patches with known vulnerabilities except in exceptional circumstances where the patch fixes more severe vulnerabilities.
- Not knowingly introduce back-doors for any reason.
- Provide reasonable notice of intent to retire or discontinue vendor support of products.

41. In addition, suppliers providing software-as-a-service (SaaS) solutions including cloud platforms must:

- Monitor their solutions for indicators of compromise.
- Ensure the system is built and configured to meet agreed service-level requirements (such as availability, mean time between failure, recovery point objective (RPO), recovery time objective (RTO), mean time to recovery, maximum tolerable downtime etc.).
- Ensure that the system has sufficient capacity to meet agreed service levels.
- Support integration with Reckitt's authentication services.

	Doc Title:	Supply Chain Cyber Security Policy	Version #	1.0
	Doc Ref #:	GLOIT-G7.3-POL130	Effective Date	20/07/2025
	Security Level:	Public	Page 6 of 9	