

1 Introduction

Husqvarna's general IT and information security requirements ("**Requirements**") for suppliers are set forth herein.

These Requirements apply to all information ("**Information**") that Husqvarna has provided to the supplier ("**Supplier**") in any form, and to all Information that Supplier has been given access to by Husqvarna or its users and representatives. This includes Information generated by Husqvarna's use of Supplier's systems or otherwise derived from Information provided by Husqvarna.

These Requirements aim to ensure:

- Confidentiality – the Information is only accessible to authorized persons.
- Integrity – the Information is accurate and safeguarded against unauthorized changes.
- Availability – the Information is available and fit for use for authorized persons when they need it.
- Traceability – changes and access to Information are securely logged to ensure traceability.

2 General requirements

Supplier shall always maintain high confidentiality and apply due care when processing the Information in accordance with these Requirements. In addition, any Information processed by Supplier shall be managed with the highest level of confidentiality as applied by Supplier in accordance with its own information security classification framework.

3 Management system

Supplier shall maintain an information security management system (ISMS) implemented in accordance with ISO 27001, ISO 27002, ISO 27701, or an equivalent standard, and shall review and update it regularly to ensure continued compliance. The ISMS shall cover all necessary administrative security controls, including policies, guidelines, procedures, suitability assessments, training, authorization processes, incident management, continuity planning, confidentiality measures and disciplinary processes regarding information security.

4 Risk management

Supplier shall maintain formal processes to systematically assess security risks related to confidentiality, integrity, availability and traceability. The assessment shall cover IT systems, applications and services provided to Husqvarna, the subcontracting chain, and the applicable information classification. Based on this assessment, Supplier shall implement appropriate security controls to ensure a level of security which is appropriate to the identified security risks, including:

- Maintaining the ongoing confidentiality, integrity, availability and traceability of Information.
- Ensuring resilience of IT systems and services processing Information.
- Restoring the availability and access to Information in a timely manner following an incident.
- Regularly testing, assessing and evaluating the effectiveness of security controls.

Supplier shall maintain documented processes and routines for managing security risks in services provided to Husqvarna. Supplier shall periodically (at least once a year) assess the security risks related to Information in the services and communicate the result of this assessment to Husqvarna.

5 Access control

Supplier shall maintain a documented access control policy covering physical, logical and remote access to facilities, networks, systems, applications, services and Information. The policy shall include an authorization process for granting and revoking user access and privileges, as well as acceptable use rules for Supplier's personnel. In addition, Supplier shall:

- Govern access to Information with role-based security.
- Have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.

- Grant access privileges based on the need-to-know and least-privilege principles.
- Use strong authentication (multi-factor) for remote access users and users connecting from an untrusted network.
- Ensure that each member of personnel has a personal, unique user ID and uses an appropriate authentication method to confirm their identity.
- Have established formal procedures for real-time logging of all access to Information made by Supplier's personnel.

Supplier shall have organizational processes in place for handling privileged access management according to best practices "Just In Time" and "Least Privileged Management" in the network, infrastructure and application layer. There shall be audit logs available for designated databases on both database and record levels. Audit logs shall log on the record level any type of process like view, add, change and delete of a record with information regarding who (user or system account), what date and time for process of the record and/or database.

6 Organization and personnel

Supplier shall maintain a security organization and information security governance framework sufficient to implement and comply with these Requirements. In particular, Supplier shall:

- designate a responsible manager for information security with the mandate to make decisions and take measures regarding these Requirements and issues in relation to Husqvarna;
- ensure all other necessary information security roles and responsibilities are designated and assigned across the organization, so that accountability for the protection of assets and information under personnel's control is clear;
- ensure that all personnel exercise due care when processing and managing Information; and
- ensure that personnel are adequately trained to maintain compliance with these Requirements.

7 Physical security

Supplier shall protect facilities where infrastructure that is used in the deliveries to Husqvarna is located and where Information is processed against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection.

Supplier shall protect goods received or sent on behalf of Husqvarna from theft, manipulation, and destruction.

Supplier's admission to Husqvarna's premises and property (such as datacenter buildings, office buildings, technical sites) is subject to the following:

- Supplier shall follow all applicable local regulations (such as regulations for "restricted areas") for Husqvarna's premises.
- Supplier personnel shall always carry an ID card or a visitor's badge visible when working within Husqvarna's premises.
- After completing the assignment, or when Supplier personnel are transferred to other tasks, Supplier shall without delay inform Husqvarna of the change and return any keys, key cards, certificates, visitors' badges and similar items.
- Keys or key cards shall be personally signed for by personnel of Supplier and shall be handled according to the written rules given upon receipt.
- Loss of Husqvarna's key or key card shall be reported without delay to Husqvarna.
- Photographing in or at Husqvarna's premises without permission is prohibited.
- Husqvarna's goods shall not be removed from Husqvarna's premises without permission.
- Personnel of Supplier shall not allow unauthorized persons access to the premises.

8 Subcontractors

Supplier shall only be entitled to engage subcontractors for the fulfilment of its undertakings subject to Husqvarna's prior written approval in each case. Supplier shall ensure that the entire subcontracting chain, as engaged and approved by Husqvarna, is subject to these Requirements to the extent needed for Supplier to comply with its undertakings. Any material changes to subcontracted services, including in the event of Supplier's intention to replace or use new

subcontractors, shall be approved by Husqvarna in writing prior to the change entering into effect.

9 Change and release management

All changes and releases to IT systems, applications or services used to store or process Information shall follow an internal change management process that protects the integrity and availability of services provided to Husqvarna. Changes shall be documented in accordance with industry good practice and made available to Husqvarna upon request.

10 Incident management and reporting

Supplier shall provide assistance, including notification, to Husqvarna when an incident occurs related to the service provided by Supplier to Husqvarna. An incident is any event that actually or potentially compromises the confidentiality, integrity, availability or traceability of information or systems, or that violates applicable security policies, standards, procedures or laws.

Supplier's assistance obligations include:

- notify Husqvarna immediately when suspecting or becoming aware of an incident. The notification shall be sent to security@husqvarnagroup.com and at least describe type and nature of the incident (e.g. security incident, personal data breach, etc.) and severity and extent of the incident (e.g. critical, severe, medium, or low);
- remediate the incident;
- submit report(s) according to this Section to Husqvarna using the contact details above;
- investigate the root cause; and
- document the incident and the remedy.

Supplier shall provide report(s) with the frequency and content requested by Husqvarna in order for Husqvarna to comply with its reporting obligation under applicable regulatory requirements. As a minimum, the reports shall include:

- a description of the incident;
- the time and date of detection of the incident;
- the period of time during which the incident has been ongoing;
- the affected services;
- the number of users affected; and
- whether anything has been communicated to users, and if so, where and when the communication took place and what information was communicated.

In addition to the reports, Supplier shall provide Husqvarna with any material information about the incident that Supplier becomes aware of.

11 Encryption, logging and malware protection

All Information shall be encrypted in transit and at rest. Cryptographic keys shall be protected physically and/or technically. Supplier shall maintain an up-to-date documented process for managing cryptographic keys and provide it to Husqvarna upon request without delay.

Supplier shall maintain a record and log of all personnel who have or have had access to the relevant IT environment. This record and log shall be stored securely to enable traceability and shall be made available to Husqvarna upon request. The IT environment shall log user identity, date and time of login and logout as well as user activities in general that are important for information security. Supplier shall document how security logs are to be analyzed. Security logs shall be available to Husqvarna upon request. In addition, records and logs shall be protected against deletion, tampering and unauthorized access.

Supplier shall ensure that effective malware and malicious code protection solutions are implemented, configured, updated and centrally managed for detection, prevention and recovery from malware and malicious code infections regarding the services.

12 Business continuity and disaster recovery

Supplier shall identify business continuity risks and take necessary actions to control and mitigate such risks. Supplier shall maintain documented processes and routines for business continuity and disaster recovery and ensure that information security is embedded into the business continuity plans. Moreover, Supplier shall periodically assess the effectiveness of its business continuity management and disaster recovery procedures, and compliance with any applicable availability requirements.

13 Compliance and auditing

Supplier shall provide Husqvarna with information security reporting sufficient to demonstrate secure, high-quality, continuously improving services, and to comply with both contractual and regulatory requirements.

Supplier shall continuously verify that only authorized persons are engaged and that the level of protection for Information remains adequately high.

Husqvarna has the right to audit Supplier's compliance with these Requirements. Audits shall take place during Supplier's regular office hours and, where necessary, on site at Supplier's location. An audit shall not be more extensive than is relevant and necessary for the specific matter under review.

Any third-party audit reports prepared in connection with Supplier's ISO certifications or SOC 2 assessments shall be shared with Husqvarna upon request.

14 Costs

Supplier is responsible for any costs it may incur to ensure compliance with these Requirements.