HUSQVARNA - IT AND INFORMATION SECURITY REQUIREMENTS

1 Introduction

Husqvarna's general IT and information security requirements for suppliers are set forth herein.

The IT and information security requirements in this document apply to all information that Husqvarna has (in any way) provided to the supplier ("**Supplier**") and information that the Supplier has been given access to by Husqvarna and/or its users and representatives, including as generated by Husqvarna's use of such systems or as otherwise derived from the information submitted by Husqvarna ("**Information**"). For the avoidance of doubt, Information shall constitute Husqvarna's confidential information.

The objective of the IT and information security requirements herein is 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

The Supplier shall always ensure high confidentiality and apply due care when processing the Information in accordance with the requirements set out herein. In addition, any Information processed by the Supplier shall be treated with the highest level of confidentiality as applied by the Supplier in accordance with its own information security classification framework.

3 Management system

The Supplier shall have and actively work in accordance with a management system for information security (ISMS) implemented in accordance with ISO 27001, 27002, 27701 or equivalent. The Supplier must, where appropriate, review and update the ISMS regularly to ensure continued compliance. In addition, the Supplier shall ensure and maintain the necessary administrative security, policies, guidelines, routines, suitability assessment, training, authorization processes, incident management, continuity planning, confidentiality, disciplinary process, etc. regarding information security.

4 Risk management

The Supplier shall have established formal processes to systematically identify and evaluate security risks related to confidentiality, integrity and availability, in particular taking into consideration the IT systems, applications, and other services, as provided to and configured for Husqvarna, the subcontracting chain, and the applicable information classification, and based on such evaluation implement appropriate security controls to ensure a level of security which is appropriate to the identified risks, including inter alia:

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of IT systems and services processing Information.
- The ability to restore the availability and access to Information in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing, and evaluating the effectiveness of security controls for ensuring the security of the processing of Information.

The Supplier shall have documented processes and routines for handling security risks within the services provided to Husqvarna. The 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

The Supplier shall have a defined and documented access control policy for facilities, sites, network, system, application and data access (including physical, logical and remote access controls), an authorisation process for user access and privileges, procedures for revoking access rights and an acceptable use of access privileges for the Supplier personnel in place. Further:

- The Supplier shall govern access to Information with role-based security.
- The Supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.
- The Supplier shall assign all access privileges based on the principles of need-to-know and least privilege.

- The Supplier shall use strong authentication (multi-factor) for remote access users and users connecting from an untrusted network.
- The Supplier shall ensure that the Supplier personnel have a personal and unique identifier (user ID), and use an appropriate authentication technique, which confirms and ensures the identity of users.

The Supplier shall have established formal procedures for real time logs of all access to Information made by the Supplier's personnel.

The Supplier shall have at least but not limited to organisational processes in place for handling privileged access management according to best practice "Just In Time" and "Least privileged management" in the network, infrastructure and application layer. There shall be audit logs available for decided databases on both the database and record level. The audit log 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 data and time for process of the record and/or database.

6 Organization and personnel

The Supplier shall have the necessary security organization and information security governance framework to implement, comply with and maintain the information security requirements. This means among other things that the Supplier shall designate a responsible manager for information security and the manager shall have a mandate to make relevant decisions/measures regarding information security requirements and information security issues in relation to Husqvarna. In addition to the responsible manager, the Supplier shall ensure all other necessary information security roles and responsibilities, to designate and assign accountability for information security across the organization to ensure that personnel apply appropriate protection to assets and information under their control. All personnel shall always exercise and apply due care when processing and managing the Information. The Supplier shall therefore ensure that its personnel are adequately trained as needed for the Supplier to ensure compliance with the IT and information security requirements set out herein.

7 Physical security

The 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.

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

The 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 local regulations (such as regulations for "restricted areas") for Husqvarna's premises when performing the assignments under the MSA.
- 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 Supplier personnel 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.
- Supplier personnel shall not allow unauthorized persons access to the premises.

8 Subcontractors

The Supplier shall only be entitled to engage subcontractors for the fulfilment of its undertakings subject to Husqvarna's prior written approval in each case. The Supplier shall ensure that the entire subcontracting chain, as engaged and approved by Husqvarna is subject to IT and information security requirements to the extent needed for the Supplier to comply with its undertakings. Any material changes to the subcontracted services, including in the event of the 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 the IT systems, applications, and/or services that are used to store and/or process Information

shall be subject to an internal change management process ensuring the integrity of and availability of the services provided to Husqvarna. Such changes shall be documented in accordance with industry good practice and shared with Husqvarna upon request.

10 Incident management and reporting

The Supplier shall provide assistance, including notification, to Husqvarna at no additional cost when an incident related to the service provided by the Supplier occurs.

The definition of incident for the purpose of this document shall mean an incident that actually or potentially could compromise the confidentiality, integrity, availability or traceability of information or information systems, or violate security policies, standards, procedures or laws.

The Supplier's obligation to provide such assistance includes, but is not limited to, that the Supplier shall:

- when suspecting or becoming aware of an incident, immediately notify Husqvarna, regardless of the time of day the incident occurs, at security@husqvarnagroup.com. To the extent it is known to the Supplier, the notification shall at least describe the type and nature of the incident (e.g. security incident, personal data breach, etc.) and the severity and the 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.

The Supplier shall provide report(s) with such frequency and content as 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, the Supplier shall provide Husqvarna with any material information about the incident that the Supplier becomes aware of.

11 Encryption, log and malicious code

All Information shall be encrypted in transit and at rest. In addition, the Supplier shall physically and/or technically protect cryptographic keys. The Supplier shall at all times have an up-to-date documented process for the handling of cryptographic key and provide this to Husqvarna upon request without delay.

The Supplier shall ensure that there is a record and log of personnel who have or have had access to the relevant IT environment. This record and log shall be stored safely so that traceability can be achieved afterwards. It shall be possible to hand over the record and log to Husqvarna on 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. The Supplier shall document how security logs are to be analyzed. The security logs shall be available to Husqvarna upon request. In addition, records and logs shall be protected against deletion, tampering and unauthorized access.

The 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

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

13 Compliance and auditing

The Supplier shall provide Husqvarna with the information security reporting required to maintain secure, high-quality, continuously improving services, and to comply with both contractual and regulatory requirements.
The Supplier shall continuously check that only authorized persons are hired and that the level of protection for Information is steady and sufficiently high.
Husqvarna has the right to audit that Husqvarna's information security regulations are complied with via audit. The audit shall take place during the Supplier's regular office hours (and if necessary, on site at the Supplier's location). The audit shall not be more extensive for the Supplier than is relevant and needed for the specific matter at hand.
Any third-party audit reports prepared in connection with the Supplier's ISO certifications, or SOC II, shall be continuously shared with Husqvarna.

14 Costs

The Supplier is responsible for any own costs it may incur as to ensure compliance with the IT and information security requirements set out herein.