HUSQVARNA - INFORMATION SECURITY REQUIREMENTS

1 Introduction

This document contains and describes Husqvarna's general information security requirements for the Supplier.

The information security requirements in this document apply to all information that Husqvarna has (in any way) provided to the Supplier and information that the Suppler has been given access to by Husqvarna. Such information will hereinafter be referred to as "Information".

The objective of the 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.

The information security requirements herein shall prevent Information from being unauthorizedly disclosed, altered, made inaccessible to authorized persons or destroyed.

2 Management System

The Supplier shall have a management system for information security implemented in accordance with ISO 27001, 27002, 27701 or equivalent. The Supplier shall actively work in accordance with its management system. The Supplier shall further 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.

The Supplier shall provide Husqvarna with the information security reporting required to maintain a secure, high-quality, continuously improving Services, and to comply with both contractual and regulatory requirements.

The Supplier shall always exercise and apply due care when processing and managing the Information.

3 Organization

The Supplier shall have the necessary security organization and information security governance framework to implement, comply and maintain the information security requirements. This means among other things that the Supplier shall have 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 have a designated contact person for information security matters and issues towards Husqvarna. The Supplier shall also have a responsible security manager for the IT systems that are intended for processing Information.

4 Subcontractors

The Supplier shall ensure that any subcontractors are subject to the same requirements regarding information security as the Supplier is towards Husqvarna. The Supplier shall inform Husqvarna if subcontractors have access to Information.

5 Security Measures

The Supplier shall always ensure that necessary information security measures are taken, implemented and documented with regard to Information. The Supplier shall, among other things:

- Implement and maintain appropriate and proportionate technical or organizational information security measures.
- Implement and maintain the principles of privacy by design and privacy by default to reduce privacy risks.
- Ensure systematic and risk-based information security work that includes e.g. risk analysis, information classifications, incident management systems, internal audits, vulnerability scans, penetration tests and internal/external audits. In addition, the Supplier shall have a systematic and documented vulnerability management process conforming with best practices for technical vulnerability management, such as those presented in section 12.6 in ISO/IEC 27002:2013.

- Ensure that Information is only handled and stored in secure premises and storage media.
- Ensure that Information is handled in IT systems that meet the relevant information security requirements herein and in accordance with industry standard.
- Ensure that personnel are trained in relevant information security requirements herein and in accordance with industry standard.
- Ensure appropriate security measures in accordance with Husqvarna's Information classification model and acceptable use policy.
- Ensure that the personnel concerned are bound by the required duty of confidentiality.
- Ensure that Information is not disclosed or shared with unauthorized persons.
- Ensure that the Supplier's premises - where Information is stored or processed - have appropriate levels of access protection.

6 Authorization

Authorization for Information may only be granted to persons at the Supplier who:

- Considered suitable to work with the information.
- Has sufficient knowledge of information security.
- Need the information for their assignment or work in the business where the Information occurs.
- Authorization shall be limited in time and only active for the period of time required for the assignment.

7 Suitability Testing

The Supplier shall test the suitability of the personnel concerned from a suitability view before personnel gain access to Information. The Supplier shall at Husqvarna's request be able to demonstrate that proper suitability tests have been carried out. Security testing means an assessment of personnel suitability comprising amongst other things (1) check of relevant grades, certificates and references (2) criminal offense register (3) verify relevant work permits (4) ensure appropriate qualifications for the assignment.

In addition, the supplier shall check and identify any reliability or loyalty issues in relation to the assignment of an individual, and to clarify whether there is an issue with the individual's participation in the assignment.

The Supplier shall notify Husqvarna of circumstances that may be of significance for the assessment of a suitability-tested person's continued suitability and reliability.

If a person, who has been tested for suitability is found to be unsuitable from a security point of view, the Supplier shall take the appropriate measures to prevent the person in question from gaining access to premises, areas or equivalent.

8 Duty of Confidentiality

Information that has been provided, added or arisen during the performance of the delivery shall even after the relationship has expired, or until Husqvarna announces something else, be covered by a duty of confidentiality.

9 Requirements for IT environments

Provisions on information security for Information in the Supplier's IT environment are as set out below:

- The Supplier may only handle Information in an IT environment that is reliable from an information security perspective. The Supplier must inform Husqvarna whether the Supplier handles Information in multi-customer IT environments and how Information is handled in order to meet the requirements for information security.
- The Supplier shall document objectives and guidelines for information security in the Supplier's IT environment.
- The Supplier shall document instructions for use, development, management and operation in the Supplier's IT environment that are intended for the processing of Information.
- The Supplier shall ensure that the Supplier's IT environment has the required authentication and authorization control system where each user is uniquely identifiable.
- 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.
- The Supplier's IT environment shall be able to detect and prevent intrusions, unauthorized access, and eavesdropping.
- The Supplier's IT environment shall always be lifecycle managed and fully supported by software and hardware manufacturers.
- If the Supplier is a company owned or controlled by operations in a country outside the European Union, the Supplier shall ensure that Information, personal data and all other information are properly encrypted and not (in any way) disclosed to such country or its authorities due to government decisions, legislation or similar. In such case, the Supplier shall also ensure that only Husqvarna has access to the encryption key and that GDPR and other applicable EU privacy laws are fully complied with regarding personal data.
- The Supplier shall ensure that files and other instructions included in electronic information transfers are encrypted at each time during the ongoing information transfer.
- The Supplier shall document routines for handling, reporting and follow-up of incidents of significance for information security in or around the IT environment. In addition, incident response plans shall follow response phases (methodology) such as defined by NIST Computer Security Incident Handling Guide (SP 800-61r2) document or later versions.
- The Supplier shall ensure that a storage medium that contains or has contained Information is only reused within the delivery by authorized personnel.
- The Supplier shall ensure that when a storage medium, which contains or has contained Information, is discarded, it shall be destroyed according to a safe method. If a storage medium is taken from the Supplier's premises, it shall be encrypted and kept under immediate supervision or stored in a way that corresponds to the level of protection that applies to the storage of the storage medium. The Supplier shall follow and apply ISO 27002 8.3 as applicable.
- If and to the extend applicable, the Supplier shall ensure that backup copies are taken regularly in accordance with a routine documented by the Supplier and stored separately from the IT environment. The backup copies shall be tested regularly.
- The Supplier shall have proper business continuity and disaster recovery plans to ensure that the Suppliers ability to provide the Services to Husqvarna is not affected in any case of IT interruption or other events natural disaster or pandemic.
- The Supplier shall assess and document the longest time that the IT environment can be out of order without significant disruptions to deliveries to Husqvarna. The Supplier shall also assess and document which backup routine is to be used if this occurs.
- The Supplier shall ensure that urgent changes that cannot follow standard routines are documented and subsequently followed up according to the routine for change management.
- The Supplier shall ensure capacity through the required capacity planning in order to anticipate and prevent capacity or performance problems in the IT environment.
- The Supplier shall, at Husqvarna's written request; provide Information in accordance with Husqvarna's instructions; and/or delete Information.
- The Supplier shall use IT equipment and software provided by Husqvarna only for the assignment and to provide the Services.
- The Supplier shall protect Husqvarna provided IT equipment and software from theft and damage. The Supplier shall report any damage or theft immediately to Husqvarna.

10 Compliance and Auditing

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.

11 Deviation reporting

The Supplier shall immediately notify Husqvarna of any events that have occurred or feared and that may affect information security with regard to Information. The Supplier's deviation reporting shall take place without delay to the contact person within Husqvarna.

The Supplier shall have documented processes and routines for handling risks within its operations. The Supplier is responsible to identify, assess and report security risks related to the provided service that affects Information.

12 Costs

The Supplier is responsible for its own costs as regards these information security requirements.