Husqvarna Group IT Supplier Security Directives

OPERATIONS, MAINTENANCE, PROCESSING, ETC., WHERE SUPPLIER PROCESSES INFORMATION OWNED BY OR IN THE CUSTODY OF HUSQVARNA

1 Scope

The Husqvarna Security Directive applies where:

1. A Supplier processes information owned by or in the custody of Husqvarna.

2 General

1. The Supplier is fully responsible for the Supplier's employees, contractors or other personnel's compliance with the Security Directives.
2. The Supplier must comply with these Security Directives and implement the measures required to ensure compliance before commencing any processing of Husqvarna information.
3. The Supplier warrants that all processing of Husqvarna's data will be compliant with these Security Directives. Upon request, the Supplier must provide Husqvarna with written confirmation of the measures taken by the Supplier to comply with these Security Directives.
4. The Supplier must notify Husqvarna at security@husqvarnagroup.com about any Security Incidents that have a probability of compromising business operations and threatening information security or a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, as soon as possible but no later than 24 hours after the Security Incident has been identified.
5. The Supplier must not allow access to Husqvarna's data or computing resources by any third party without prior written approval from Husqvarna.
6. Upon termination of the data processing services, the Supplier must return or destroy (as determined by Husqvarna) any Husqvarna data and any copies thereof, and confirm in writing the destruction of the data.

3 Security governance and policies

1. The Supplier must maintain a security policy that:
   - provides guidance to its personnel to ensure the confidentiality, integrity and availability of Husqvarna information whether processed in Information and Communications Technology (ICT) solutions of the Supplier or those of Husqvarna , and

- provides guidance regarding the steps to take in the event of a suspected or actual Security Incident involving the unauthorized disclosure, loss, or theft of Husqvarna confidential data or Information
- The policy must be complemented by an Information Security Management System (ISMS) covering the areas set forth in the ISO 27001:2013 or later.
- The policy and the ISMS must be reviewed and assessed for its effectiveness at least annually and is subject to audit by Husqvarna upon request.

3.1 Information Security Risk management

1. The Supplier must maintain a documented ongoing Risk Management Process for the identification, assessment and treatment of risks related to the confidentiality, integrity and availability of information, IT-systems and services related to Husqvarna processed data and computing facilities.

3.2 Risk management for the processing of the personal data

1. The Supplier must identify, evaluate and treat risks related to the privacy, rights and freedoms of data subject, and based on such evaluation implement appropriate technical and organizational measures to ensure a level of information security which is appropriate for the risk of the specific processing. Such measures include as appropriate,
    a) Data minimization
    b) The ongoing maintaining confidentiality, integrity, availability and resilience of processing systems and services
    c) The pseudonymizing and encryption of personal data
    d) The ability to restore availability and access to Husqvarna's data in a timely manner in the event of a physical or technical incident
    e) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing
    - The Supplier must have documented processes and routines for handling risks when processing Personal data on behalf of Husqvarna.
    - The Supplier must periodically assess the risks related to information systems and processing, storing and transmitting Personal data.

4 Organization of Information Security

1. The Supplier must have a documented and implemented security governance system, organization and capability that contains all the necessary resources to perform the obligations set forth in these Security Directives. The Supplier must collaborate with Husqvarna to effectuate, with adequately skill and trained personnel, what is set forth in these Security Directives, e.g., contribute to risk analyses, disaster recovery drills, etc., as applicable.
2. The Supplier must appoint at least one person who has the appropriate security competence and who has an overall responsibility for implementing the Security Directives and who will be the contact person for the Husqvarna Security function .

5 Human Resource Security

1. The Supplier must ensure that all personnel involved with the processing of Husqvarna data or connected with the Husqvarna's systems or networks (including the copies of Supplier's proprietary technology and third party technology installed thereon) that directly or indirectly support the processing of Husqvarna's information meets established security criteria and has been subject to appropriate screening and background verification and are made aware of and are required to adhere to security policies and security practices before handling any Husqvarna data or information.
2. Supplier must at all times maintain a current list of personnel that processes Husqvarna information and on request provide Husqvarna with an unique identifier of the physical person e.g. Userid, email address.
3. The Supplier must provide periodical security awareness training to relevant Supplier personnel categories. Such training include:
   - how to handle customers information securely (i.e. the protection of confidentiality, integrity and availability of the information);
   - why information security is needed to protect customer´s information and systems;
   - the common types of security threats (such as identity theft, malware, hacking, information leakage and insider threat);
   - the importance of complying with information security policies and applying associated standards/procedures;
   - personal responsibility for information security, e.g., reporting actual and suspected Security Incidents.
4. The Supplier must have their IT and information security staff sign Non-Disclosure Agreement(s)/confidentiality clause(s) or have such terms incorporated into their employment contracts prior to being granted access to Husqvarna applications, systems or networks. Such agreements or clauses must be in effect also outside normal working hours and premises, and continue at least five years after employment has ended.
5. The process for dealing with associates non-compliance must be defined and documented. The process must be fair and objective.

6 Assets management

1. Supplier must identify information, people and technology assets necessary for the delivery in scope. Information assets include but are not limited to IT systems, backup and/or removable media containing sensitive information, access rights, software and configuration. Assets must be documented in an accurate, consistent and up-to-date assets inventory. For each asset its classification and ownership must be assigned. The Supplier must keep an updated list of Husqvarna’s data processed, identifying the processed data, storage details, such as asset name, location etc.

7 Access control

1. The Supplier must have a defined and documented access control policy for facilities, networks, IT-systems, applications and information/data (including physical, logical and remote access). The Supplier must have processes for authorization and approval of user access and privileges**.**
2. The supplier must have a formal and documented user registration and de-registration process implemented to enable assignment of access rights to physical persons. Assignment of access privileges must be based on the principle of legitimate business need and principle of least privilege. The Supplier must use strong authentication (multi-factor) for remote access and connecting from untrusted networks and users working with system admin privileges.
3. The Supplier must ensure that the Supplier Personnel has personal and unique identifier(s) (user ID) and that one and the same user-ID is not used for both system administration and office automation tools, e.g., surfing the web, reading email, using word processors.

8 Cryptography

1. The Supplier must have a defined and documented cryptography policy. Use of cryptography must be implemented and monitored by, skilled and knowledgeable people to ensure the secure use of defined processes, crypto -keys and -algorithms to effectively rendering information and personal data unintelligible to any person not in possessions of decryption keys.

9 Physical and environmental security

9.1 Secure areas

1. Supplier must protect information processing facilities from where services are provided and/or where Husqvarna assets are kept or processed, by use of security perimeters providing sound protection from environmental, intentional and unintentional threats. Such protection shall include admission for authorized persons only and the maintaining of an accesses ledger/log and the wearing of visible badge. 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 key or key card shall be reported without delay to the security function of the Supplier or to the Buyer depending on who issued the lost key or key card.
2. The Supplier must protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

9.2 Equipment

1. Power and telecommunication cabling carrying data or supporting information services must be protected from interception, interference and damage. Equipment must be protected from power failures and disruptions by failures in

supporting utilities. Equipment and supporting infrastructure must be appraised regularly for the capacity to meet business growth.

2. Supplier must ensure that all equipment containing storage media that holds or may have held Husqvarna information is cleansed such that information is irretrievable permanently erased before equipment is reused for other purposes or decommissioned.

10 Operations security

1. The Supplier must have a change management system in place for changes to business processes, Information Processing Facilities and systems. The change management system must include planning, tests and reviews before changes are implemented, such as procedures to handle urgent changes, fallback procedures to aborting and recover from failed changes, logs that show, what has been changed, when and by whom.
2. The supplier must keep operational environments separated from development and testing environments. Husqvarna information must not be processed for testing, development, etc. unless specifically agreed in writing.
3. The Supplier must implement malware protection and recovery controls to ensure that any software used for Supplier's provision of the deliverables to Husqvarna is protected from malware.
4. The Supplier must create and maintain backup copies of critical information and system images. Restorability of back-up copies must be regularly verified.
5. The Supplier must maintain a complete and accurate log and monitor activities, such as creating, reading, updating and deletion of processed data, as well as exceptions, faults and information security events and regularly review these. Furthermore, the Supplier must protect and store (for at least six (6) months) log information, and on request, provide monitoring data to Husqvarna. Anomalies / incidents / indicators of compromise must be reported according to the Data Breach Reporting section.
6. The Supplier must manage vulnerabilities of all relevant technologies such as operating systems, databases and applications proactively and in a timely manner. Hardware or software for that security patches are not provided must not be used. Processes and systems must be devised such that the timely applying of security patches is feasible.
7. The Supplier must establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

11 Communications security

1. The Supplier must have implemented network security controls such as segregating networks, remote access using strong means of authentication, controlled internetwork traffic policies.
2. The Supplier must have implemented controls to allow electronic messages to be properly protected, e.g., encryption in transit, authentication of systems and email-domains.

12 System acquisition, development and maintenance

1. The Supplier must include security as part of their software development lifecycle, observing best practices, e.g., OWASP top-ten.
2. The Supplier must verify security functionality during development in a controlled environment.

13 Supplier relationships

1. The Supplier must ensure their suppliers adhere to this Security Directive in its agreements with sub-suppliers that perform tasks assigned under the Agreement.
2. The Supplier must regularly monitor, review and audit sub-supplier‘s compliance with the Security Directives.
3. The Supplier must, at the request of Husqvarna, provide Husqvarna with evidence regarding sub-supplier’s compliance with the Security Directives alternatively the sub-supplier provides the evidence/report directly to Husqvarna.

14 Security incident management / Data Breach Reporting

1. Upon discovering any suspected or actual Security Incident involving the unauthorized disclosure, loss, or theft of Husqvarna confidential data or Information (a “Data Security Breach”), the Supplier must:
   a) Take actions to stop the breach and to minimize damage.
   b) Promptly (as soon as possible but no later than 24 hours of discovery) notify Husqvarna of the breach, its properties and handling. See section 2 above for contact details.
   c) Fully cooperate with Husqvarna to provide all information in a timely manner and must fully cooperate with Husqvarna, as directed by Husqvarna, to make any notifications required by applicable law.
   d) Fully cooperate with Husqvarna to identify a root cause and remediate any Data Security Breach at their sole cost.
   e) Designate an individual who will serve as the Supplier ’s ongoing single point of contact for purposes of addressing issues with respect to the use and security of Husqvarna confidential information during the term and following the termination or expiration of these standards. Such an individual must be accessible to Husqvarna on a 24 hour basis. The Supplier must ensure that this individual can obtain relevant information specific to any incidents within 48 hours. This individual is to also have access to or direct knowledge of Supplier’s network architecture and information technology system.

15 Business continuity management

1. The Supplier must identify business continuity risks and take necessary actions to control and mitigate such risks, e.g., maintain business continuity and disaster recovery plans.
2. The Supplier must have documented and regularly rehearsed processes and routines for business continuity.
3. The Supplier must ensure that information security is embedded into the business continuity plans such that information security control objectives are met also during disasters and crisis.
4. The Supplier must periodically assess the efficiency of its business continuity management, and compliance with applicable availability requirements.