| | Effective Date: May 7, 2018 | Last Revision Date: May 7, 2018 |
|---|---|---|
| HORIZON GLOBAL | Approved by: CIO | |
| | Page 1 of 3 | |

# Title: Supplier Information Security Requirements Policy

**DEFINITIONS:** The following terms shall have the meaning set forth below for purposes of this Supplier Information Security Requirements Policy (the "Policy").

**Horizon Global Information** means any data or information concerning Horizon Global Corporation, its affiliates, subsidiaries, divisions, employees, clients, successors or permitted assigns (collectively, "Horizon Global") that is provided to or obtained by Supplier in connection with the negotiation and execution of the underlying agreement between the parties or the performance of Supplier's obligations under the agreement, including any such data and information that either (i) is created, generated, handled, collected, processed or disposed of by Supplier in the performance of Supplier's obligations under the agreement or (ii) resides in or is accessed through Horizon's Information Systems or Supplier's Information Systems; as well as any data and information derived from the foregoing. Horizon Global Information includes, but is not limited to, all Horizon Confidential Information as defined in the Confidentiality and Compliance Agreement for Suppliers.

**Information Systems** means all hardware, software, operating systems, database systems, software tools and network components used by or on behalf of Horizon to receive, maintain, process, store, access or transmit Company Information.

**SCOPE**:

This Policy applies to all Suppliers, its parent companies, affiliates and subsidiaries, all present and future officers, directors, representatives, agents, employees, assignees, successors, beneficiaries and any and all personnel (collectively, the "Supplier") which use, process, access, hold or transmit the Horizon Global Information. The Policy also applies to all independent contractors, personnel, third-party suppliers and service providers working with or for Supplier who use, process, access, hold or transmit the Horizon Global Information.

**PURPOSE**:

Horizon Global is committed to protecting Horizon Global Information. The purpose of this Policy is to define the framework for ensuring the confidentiality, security, integrity and availability of Horizon Global Information and set forth Supplier guidelines for protecting Horizon Global Information.

**SUPPLIER INFORMATION TECHNOLOGY REQUIREMENTS AND SECURITY MEASURES:**

All Suppliers must comply with the following Information Technology ("IT") requirements and the following security measures:

1. Supplier must have a comprehensive IT Security program in place that meets the ISO27001/27002 standards and is reviewed at a minimum on an annual basis.

2. Proliferation of Horizon Global information is controlled and monitored across Supplier's IT environment.

3. Only authorized users are allowed access to Horizon Global Information (in both electronic and paper form).

4. Supplier must notify Horizon Global if it shares or provides access to Horizon Global Information to any independent contractor or third-party supplier.

5. Supplier must ensure that any transmission of Horizon Global Information outside of Supplier's network or internally by wireless is encrypted and protected, including, but not limited to, information sent via email.

6. Supplier must ensure that its network is adequately protected from external threats and must perform network penetration tests at a minimum on an annual basis and mitigate any vulnerabilities found because of the tests.

7. Supplier must implement an Incident Response and Data Breach process which includes notifying Horizon Global if there is a breach of Horizon Global Information from Supplier's or any other third party's IT environment.

8. Supplier must protect Horizon Global Information residing on mobile/smart devices through encryption where possible and perform adequate backups in the event the device is lost or stolen.

9. If Supplier is connecting to Horizon Global's network, Supplier will work with the Horizon Global IT department to setup properly secured network connections.

10. Supplier will take all necessary precautions to wipe Horizon Global Information from its hardware before the disposal of the hardware.

11. Upon written request by Horizon Global, Supplier will delete all Horizon Global Information from its IT environment.

12. Supplier must notify Horizon Global if it is in possession of any Horizon Global employee Personal Health Information (PHI) or Personally Identifiable Information (PII).

13. Supplier must maintain an effective form of data retention and backup procedure that insures that product and testing information for all Horizon Global products is stored in a safe location and is readily accessible electronically.

14. Any trans-border movement of Horizon Global Information must comply with all governing local, state, national and international laws.

15. Any remote access into Supplier's network must use a multi factor login protocol.

16. Supplier must maintain security policies relating to the storage, access and transportation of records containing personal information outside of business premises.

17. Supplier must maintain reasonable restrictions of physical access to Horizon Global Information in the possession of Supplier that contain personal information, and such records and data must be securely stored in locked facilities, storage areas or containers.

18. Supplier must maintain security procedures to prevent former employees from accessing Horizon Global Information, including, but not limited to, records containing personal information.

19. Supplier must assign unique identifications plus passwords, which are not shared and are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

20. Supplier must maintain reasonably up-to-date firewall protection and operating system security patches on all Supplier devices with internet access.

21. Supplier must maintain reasonably up-to-date versions of endpoint protection software on all Supplier computers.

22. Supplier must restrict access to records and files containing personal information to those who need such information to perform their job duties.

23. Supplier shall educate its employees on external and internal security threats to the company data.

Horizon Global reserves the right to audit, or hire a third party to audit, the security of Horizon Global Information and compliance with this Policy. Horizon Global further reserves the right to cease doing business with Supplier if it is found to be non-compliant with this Policy, without any liability resulting from such termination. Supplier agrees to comply with all requests for information from Horizon Global or its third-party auditor to confirm compliance.