GE Gas Power

GE Gas Power Supply Chain Security

WHITEPAPER

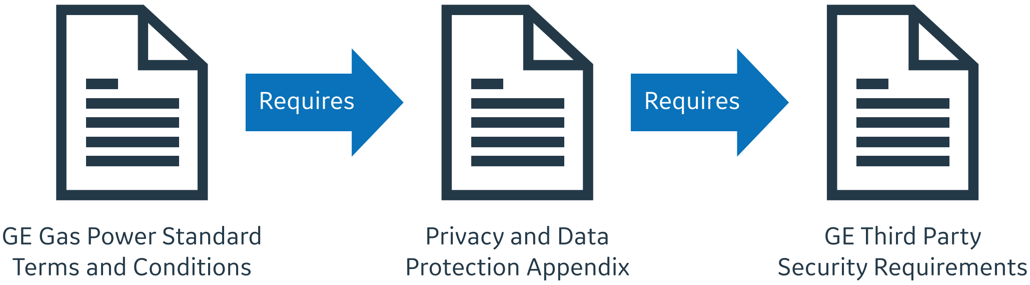
Introduction

GE Gas Power has a mature, robust security program for its corporate IT systems and the products we sell to our customers. However, we understand that the security of our systems and products also depends on our supply chain – the companies that provide essential goods and services to operate our business. GE Gas Power manages the security of our supply chain through two primary mechanisms:

1. We apply cybersecurity requirements on our suppliers to help ensure that they commit to follow industry standard security practices, such as NERC CIP requirements.
2. We assess our suppliers' security posture through the 3rd Party Security (3PS) process, which determines the level of risk a new supplier may face from a cyber-security standpoint.

In addition, GE Gas Power meets the vendor responsibilities specified in NERC CIP 013.

Terms and Conditions



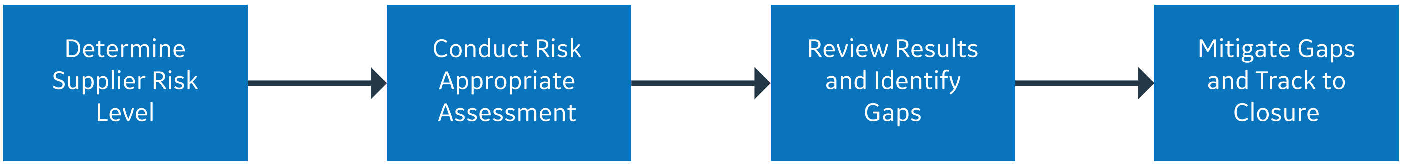
GE Gas Power Standard Terms and Conditions → Requires → Privacy and Data Protection Appendix → Requires → GE Third Party Security Requirements

GE uses a *Standard Terms of Purchase* when conducting business with its suppliers. This document mandates suppliers to follow the *Privacy and Data Protection Appendix*, which requires compliance with security standards, including:

- Promptly notifying GE Gas Power in case of a cybersecurity incident
- Providing appropriate audit and vulnerability assessment procedures
- Complying with the *GE Third Party Security Requirements* document, which contains an extensive list of security controls for the supplier's enterprise IT systems and the products they sell to GE Gas Power. Here are some examples of product security requirements:
  - Suppliers must incorporate secure software development best practices when developing their products, such as performing security design reviews, utilizing secure coding practices, and performing risk-based testing.
  - Suppliers must have a vulnerability management plan to identify and mitigate vulnerabilities in their products.
  - Suppliers must provide a mechanism, such as digital signatures, to allow users to verify the integrity of supplied software.

Through these universal terms and conditions, GE Gas Power requires its suppliers to meet consistent security requirements and controls.

3rd Party Security (3PS) Process


Determine Supplier Risk Level
Conduct Risk Appropriate Assessment
Review Results and Identify Gaps
Mitigate Gaps and Track to Closure

The 3PS process employs a risk-based approach to evaluating the security practices of our suppliers. The type of assessment conducted depends on the nature of our relationship with the supplier, such as the type of data we provide and the products we procure.

Lower risk suppliers receive a quicker assessment based on open source intelligence. Higher risk suppliers are required to complete a self-assessment questionnaire that documents security best practices for a range of subject areas, including data protection, cloud, privacy, secure development, and OT/Manufacturing. The questions and controls are based on widely adopted security standards including ISO 27001, NIST 800-53, NIST 800-171, NERC-CIP 013, and IEC 62443.

Once the supplier completes the questionnaire, responses are reviewed by the 3PS team. Identified gaps are highlighted and the supplier is asked to provide a corresponding remediation plan. The 3PS tracks open items until they are completed, and only upon closing all open items is the assessment completed.

NERC CIP 013

NERC CIP is a federally regulated set of cybersecurity requirements for electric utilities in North America. NERC CIP 013 specifies numerous supply chain security requirements and places six requirements on vendors, all of which are satisfied by GE Gas Power.

Requirement Number	Requirement Text	GE Gas Power Compliance
013-1 R1.2.1	Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	GE Gas Power has a comprehensive incident response program that notifies customers of incidents that affect their data and products
013-1 R1.2.2	Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	GE Gas Power's incident response program works with its customers as necessary to respond to an incident
013-1 R1.2.3	Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;	GE Gas Power terminates access and notifies customer that access is no longer needed
013-1 R1.2.4	Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;	GE Gas Power maintains a vulnerability management program and discloses newly discovered vulnerabilities to customers through the process of responsible disclosure
013-1 R1.2.5	Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and	Software is digitally signed to allow for integrity verification
013-1 R1.2.6	Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	GE Gas Power uses industry standard security controls for remote access and verifies the use of such controls with its customers