Control Guidance

Top 5 Data Loss Prevention Findings

Document Control Information

Version	1.2
Revision	1
Issued	26/11/2025
Annual Review	Q4
Process Owner (s)	Abhinandan Kumar
Program Owner	Abhinandan Kumar
Approved by	Abhinandan Kumar
Functional Team	GE Vernova Third Party Security
Document Classification	GE Vernova Public

Version Control

The Process owner(s) are responsible for maintaining the master copy of the document and keeping the document updated annually to incorporate any changes in the process.

Revision Number	Date of Issue	Author(s)	Reviewer(s) /Approver(s)	Brief Description of Changes
1	7/5/2022	Aaron Kunec	David Prescott	Final Draft
2	26/11/2025	Aakash Singhal	Abhinandan Kumar	Updated for GE Vernova

Data Loss Prevention – 1

Risk Rating: **High**

<table>
<tr><td colspan="2"><b>Control Question</b> - Is Uniform Resource Locator (URL) web filtering in place to block access to high-risk sites and non-sanctioned file sharing applications?
Note: High-risk sites can include but are not limited to peer-to-peer file sharing sites and sites hosting adult/mature content.
<b>What is the risk?</b> In addition to leaving your organizations network exposed to websites hosting malware and inappropriate content, not having a URL Web filter can leave your organization exposed to intentional or accidental exfiltration of sensitive data.
<b>What we are looking for:</b> Statement attesting that your organization has an established documented policy to block access to high-risk sites as well as non-approved file sharing applications via the use of technical controls such as Uniform Resource Locator (URL) web filtering, white-listing company approved web sites or DNS filtering.</td></tr>
<tr><td><b>Acceptable Compensating Controls</b></td><td>Supply a statement attesting to the following points.
• GEV data is segregated from the general network and is controlled via access control lists
• GEV data is encrypted at rest and in transit.
• A data retention policy is in place stating that GEV (Or customer) Data is not to be saved locally on company laptops/desktops</td></tr>
</table>

Data Loss Prevention – 2

Risk Rating: **High**

<table>
<tr><td colspan="2"><b>Control Question</b> - Is a host-based data loss prevention (DLP) solution implemented on all laptops/desktops within your organization? Examples of DLP solutions include but are not limited to Digital Guardian or Symantec DLP.
<b>What is the risk?</b> Not having a data loss prevention system monitoring your endpoints can leave your organization open to data theft. Additionally, modern host based DLPs can be enabled to help with disk hygiene by tracking and removing sensitive information that may been unintentionally saved locally
<b>What we are looking for:</b> Statement attesting that your organization has implemented a host-based data loss prevention (DLP) solution on all devices used to access/process GEV data.</td></tr>
<tr><td><b>Acceptable Compensating Controls</b></td><td>Supply a statement attesting to the following points.
• GEV data is segregated from the general network and is controlled via access control lists
• All USB ports are blocked on workstations that access, or process GEV sensitive data.
• A data retention policy stating that GEV (Or customer) data is not to be saved locally on company laptops/desktops</td></tr>
</table>

Data Loss Prevention – 3

Risk Rating: **High**

Control Question - Is there a network based DLP solution implemented to monitor and control inbound and outbound email, network, and application traffic?

What is the risk? Not having a DLP solution monitoring email can leave your origination open to the accidental, internal, or malicious data theft.

Some examples include...

- Internal bad actors exfiltrating customer data
- Message with sensitive data sent to incorrect personnel
- File with sensitive data attached to incorrect email message
- Employee not realizing a file contains sensitive data and sending it via email

Additionally, **e**mail data loss prevention software should scan all incoming messages to look for links that could indicate a phishing attach.

What we are looking for: Statement attesting that your organization has implemented a network-based data loss prevention (DLP) solution to monitor and control inbound and outbound emails, network, and application traffic containing GEV data.

Acceptable Compensating Controls	Supply a statement attesting to the following (all points must be attested to) … • GEV data is segregated from the general network and is controlled via access control lists • GEV data is encrypted at rest and in transit. • Data retention policy stating that GEV Data is reviewed annually and deleted if data is no longer in use.

Data Loss Prevention - 4

Risk Rating: **High**

Control Question - Are USB ports on all workstations that access, process, or store GEV sensitive data blocked?

What is the risk? Enabling the use of, or not blocking data labelled as sensitive from being exported via USB ports can leave your organization exposed to data theft as well as leaving an open avenue for malware to traverse.

What we are looking for: Statement attesting that USB access on all workstation that access, or process GEV Data have been blocked

Acceptable Compensating Controls	Supply a statement attesting to the following (all points must be attested to) … • GEV data is segregated from the general network and is controlled via access control lists • Company workstations have a host based DLP solution enabled. • A data retention policy stating that GEV (Or customer) data is not to be GEV data saved locally on company laptops/desktops

Data Loss Prevention – 5

Risk Rating: **High**

Control Question - Is Uniform Resource Location (URL) filtering in place to block access to personal email and online storage sites such as Dropbox and Google drive? **What is the risk?** Not having a URL filter in place to block personal email accounts or unapproved online storage can leave your organization exposed to intentional or accidental exfiltration of sensitive data. **What we are looking for:** Statement attesting that your organization has enabled Uniform Resource Location (URL) filtering to restrict access to personal email and online storage sites such as Dropbox and Google drive.	
Acceptable Compensating Controls	Supply a statement attesting to the following (all points must be attested to) … • GEV data is segregated from the general network and is controlled via access control lists • A data retention policy stating that GEV (Or customer) Data is not to be saved locally on company laptops/desktops • GEV data is encrypted at rest and in transit.