**Control Guidance**

**Top 10 Physical Security Findings**

**Document Control Information**

|  |  |
| --- | --- |
| Version | 1.1 |
| Revision | 1 |
| Issued | 7/5/2022 |
| Annual Review | Q4 |
| Process Owner (s) | Aaron Kunec |
| Program Owner | Aaron Kunec |
| Approved by | David Prescott |
| Functional Team | GE Power-IT-Security Third Party |
| Document Classification | GE 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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Document Control Information**

|  |  |
| --- | --- |
| Version | 1.1 |
| Revision | 1 |
| Issued | 7/5/2022 |
| Annual Review | Q4 |
| Process Owner (s) | Aaron Kunec |
| Program Owner | Aaron Kunec |
| Approved by | David Prescott |
| Functional Team | GE Power-IT-Security Third Party |
| Document Classification | GE 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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Physical Security – 2**

Risk Rating: **Critical**

**Note: A statement alone is not sufficient for Control Questions with a Risk Rating of Critical. Attaching evidence is required to meet the control standards**

|  |  |
| --- | --- |
| **Control Question** - Are all servers and network equipment used to store and/or access GE data kept in a secure room with the following controls: 1. Additional access control mechanisms (e.g. badge, biometrics, pin, etc.) on entry doors, 2. Rooms are located on the interior of the building with no windows, unless safeguards are in place to prevent shattering, and 3. Telecommunications equipment, cabling and relays receiving data or supporting services are hidden from view to deter interception or damage? Note: If GE data is only stored or processed in a cloud environment, respond to this control based on your organization's validation that appropriate security controls are in place at your cloud hosting provider. If all aspects above are not implemented, please answer "No" and indicated which aspects are not adhered to.  **What is the risk?** Having an access-controlled data center or server room with no widows can lower the risk of data theft and help prevent unintentional or Intentional damage to your equipment. Additionally, this will help provide a climate-controlled environment to keep systems at a cooler temperature so to prevent service interruptions.  **What we are looking for:** Evidence attesting that all access control mechanisms mentioned are in place and currently in use.   1. Additional access control mechanisms (e.g. badge, biometrics, pin, etc.) on entry doors 2. Server Rooms are located on the interior of the building with no windows, unless safeguards are in place to prevent shattering 3. Telecommunications equipment, cabling and relays receiving data or supporting services are hidden from view to deter interception or damage? | |
| **Acceptable Compensating Controls** | Supply evidence attesting to the following points.   * Additional mechanism (e.g., Lock and Key), and who will have access to the mechanism. * Alarm system on premise.   Or   * No server room is needed as data is housed in a cloud solution (please include name of cloud solution). |

**Physical Security – 3**

Risk Rating: **High**

|  |  |
| --- | --- |
| **Control Question** - For all facilities used to access, process, transmit, and/or store GE data, are security cameras implemented to monitor the perimeter, entry/exit points, and the interior of the facility? Note: If GE data is only stored or processed in a cloud environment, respond to this control based on your organization's validation that appropriate security controls are in place at your cloud hosting provider.  **What is the risk?** Not having security camaras monitoring your data center hinders your organization’s ability to conduct a timely and successful investigation in the event of an unauthorized access attempt or physical breach.  Note: The presence of security cameras can also act as a deterrent. Like security alarms, if an unauthorized person knows that cameras are recording their actions, they may be less inclined to attempt to gain entry.  **What we are looking for:** Statement attesting that your organization has security cameras monitoring your data center or server room that houses GE data. | |
| **Acceptable Compensating Controls** | Supply a statement attesting to the following points.   * Two factor mechanisms (something you know and something you have) e.g., Lock and Key and Key code pad * Documented process for tracking which employees have authorization to your data center or server room that houses GE data.   Or   * No server room is needed as data is housed in a cloud solution (please include name of cloud solution). |

**Physical Security – 4**

Risk Rating: **High**

|  |  |
| --- | --- |
| **Control Question** - Are security camera recordings retained for at least 30 days?  **What is the risk?**  A physicalunauthorized access attempt or a successful breach to your data center can go undetected for days or weeks. Not retaining your security camera footage can hinderyour organization’s ability to conduct a thorough investigation.  **What we are looking for:** Statement attesting that organization retains security camera footage for at least 30 days. | |
| **Acceptable Compensating Controls** | Supply a statement attesting to the following point.   * Documented process for tracking which employees have authorization to your data center or server room that houses GE data.   Or   * No server room is needed as data is housed in a cloud solution (please include name of cloud solution). |

**Physical Security – 5**

Risk Rating: **High**

|  |  |
| --- | --- |
| **Control Question** - For all facilities used to access, process, transmit, and/or store GE data, is access controlled by a security guard, mantrap, or other means when entering the facility? Note: If GE data is only stored or processed in a cloud environment, respond to this control based on your organization's validation that appropriate security controls are in place at your cloud hosting provider.  **What is the risk?** Piggybacking is a common tactic used by unauthorized individuals to access restricted areas. Having a Security Guard or Mantrap in place can make piggybacking impossible.  **What we are looking for:** Statement attesting | |
| **Acceptable Compensating Controls** | Supply a statement attesting to the following points   * GE data is stored in a room secured with a mechanism (Lock & Key, Keypad, Biometrics, etc.) that is limited to approved personnel only * Documentation is in place stating which individuals to facilities that store GE data * A periodic audit is conducted to review who has access to the security mechanism. * Security camera recording your data centers entry way.   Or   * No server room is needed as data is housed in a cloud solution (please include name of cloud solution). |

**Physical Security – 6**

Risk Rating: **High**

|  |  |
| --- | --- |
| **Control Question** - Are identification badges issued to all employees, contractors, and visitors and always worn? Note: If GE data is only stored or processed in a cloud environment, respond to this control based on your organization's validation that appropriate security controls are in place at your cloud hosting provider.  **What is the risk?** Curious customers or even competitors look for distracted employees to gain access to restricted areas. Not using ID badges makes identifying people who have the correct authorization more difficult.  **What we are looking for:** Statement attesting that identification badges are assigned to all employees and guests. | |
| **Acceptable Compensating Controls** | Supply a statement attesting to the following points   * Organization employees less than 10 people * Guests are not permitted on site   Or   * Paper sign in log is used for employees and visitors |

**Physical Security – 8**

Risk Rating: **Critical**

**Note: A statement alone is not sufficient for Control Questions with a Risk Rating of Critical. Attaching evidence is required to meet the control standards**

|  |  |
| --- | --- |
| **Control Question** - Are all physical documents that contain GE data/information kept in a locked office, cabinet, or other location which is locked, and access restricted to authorized personnel only? Note: If physical documents containing GE data/information are not stored by your organization, select "Not Applicable" and add comment that physical documents are not stored.  **What is the risk?** Having an access-controlled data center or server room with no widows can lower the risk of data theft and help prevent unintentional or Intentional damage to your equipment. Additionally, this will help provide a climate-controlled environment to help keep systems at a cooler temperature so to prevent service interruptions.  **What we are looking for:** Evidence (photo or other documentation) attesting that physical document are kept under lock and key. | |
| **Acceptable Compensating Controls** | Compensating Controls are not permitted for this Control Question. |

**Physical Security – 9**

Risk Rating: **High**

|  |  |
| --- | --- |
| **Control Question** - Are mechanisms in place to notify, investigate, and address potential physical security incidents such as physical intrusion or a stolen asset?  **What is the risk?** Not being able to alert authorities in a timely manner increases the success of burglars stealing your physical assets (Servers, laptops, computers, etc..).  **What we are looking for:** Statement attesting that your Incident Management Plan includes investigating and addressing physical security Incidents. | |
| **Acceptable Compensating Controls** | Supply a statement attesting to the following points   * Security Camaras are installed and retaining at least 30 days of footage * An asset inventory is audited and accounted for on a 6-month bases * Locking or access control mechanism on all permitter points of egress. * Locking or access control mechanism applied to data centers (does not not apply if cloud solution is used in-leu of a data center) |

**Physical Security – 10**

Risk Rating: **High**

|  |  |
| --- | --- |
| **Control Question** - If all facilities used to access, process, transmit, and/or store GE data are not staffed 24x7x365, are alarms installed for off-hour access monitoring? Note: If all facilities used to access, process, transmit, and/or store GE data are staffed 24x7x365, select "Not Applicable" and add comment that all facilities are staffed 24x7x365.  **What is the risk?** Burglary are one of the top causes of revenue loss for businesses. These incidents make up 13.6% of property crimes, but businesses are four times more likely than homes to be burglarized. For your business, this means that your customer data and asset inventory are more at risk than you may realize. You not only risk losing assets and data, but risk property damage as well. By having eyes on your business 24x7x365, you can increase your chance of being compensated for these incidents.  **What we are looking for:** Statement attesting that a security alarm is installed and in use. | |
| **Acceptable Compensating Controls** | Supply a statement attesting to the following points   * Security Camaras are installed, and video is retaining for at least 30 days. * An asset inventory is audited and accounted for on a 6-month bases * Locking or access control mechanism on all permitter points of egress. * Locking or access control mechanism applied to data centers |

**Physical Security – 11**

Risk Rating: **High**

|  |  |
| --- | --- |
| **Control Question** - If facilities used to access, process, transmit, and/or store GE data are shared with other occupants (e.g. co-located data center), are protective mechanisms implemented between occupants to prevent unauthorized access to your organizations physical equipment (e.g. locked cage, badge access, etc.)?Note: If facilities used to access, process, transmit, and/or store GE data are not shared with other occupants, select "Not Applicable" and add comment stated that facilities are not shared.  **What is the risk?** Segregation of serves is an obstacle that makes lateral movement difficult and helps isolate security zones. Whether it be a malicious attack or technical fault, proper segregation of IT environments can limit the spread to other internal areas, reducing the potential impact.  **What we are looking for:** Statement attesting that your organization has segregated security zone in place (locked cages, badge access, security camaras). | |
| **Acceptable Compensating Controls** | Compensating Controls are not permitted for this Control Question. |

**Physical Security – 12**

Risk Rating: **High**

|  |  |
| --- | --- |
| **Control Question** - Are physical access rights reviewed on an annual basis (at a minimum) and updated as needed to ensure physical access to all facilities used to access, process, transmit, and/or store GE data is restricted to authorized personnel? Note: If GE data is only stored or processed in a cloud environment, respond to this control based on your organization's validation that appropriate security controls are in place at your cloud hosting provider.  **What is the risk?** A periodic physical access rights review can help ensure that only authorized personnel will have access to need-to-access areas. Mitigating or Investigating thefts or the malicious destruction of property and data can become difficult without keeping up-to-Date authorization records.  **What we are looking for:** Statement attesting to an annual review of the physical access rights of your employees for your office, server room, and data center | |
| **Acceptable Compensating Controls** | Supply a statement attesting to the following points   * Statement attesting to how many employees will have access to the data center or server room where GE data is housed * Statement attesting to any physical controls to the data center or server room where GE data is housed   Or   * No server room is needed as data is housed in a cloud solution (please include name of cloud solution). |