## Security Tool Kit

### Security Controls Matrix for Data Classification

**INSTRUCTIONS**

The Security Controls Matrix for Data Classification is used to determine where in the Data Classification Policy the system falls based on the type of information on the system (Public, Official Use, Confidential) and the type of system itself (Desktop, Departmental Server, Enterprise System). This matrix states the minimal security requirements for the system.

At a minimum, all departmental servers and enterprise systems must have their Data Classification level clearly stated in the System Checklist under the System Data Characteristics section.

<table>
<thead>
<tr>
<th>Public</th>
<th>Desktop Technical</th>
<th>Operational</th>
<th>Department Technical</th>
<th>Operational</th>
<th>Enterprise Technical</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Determine how the system is to identify and authenticate each user.</td>
<td>1. Use antivirus and updated definitions 2. Use operating system and software patches 3. User should complete the on-line security and awareness training.</td>
<td>1. Determine how the system is to identify and authenticate each user. 2. Determine what logical and physical access controls should be in place.</td>
<td>1. Addresses documentation requirements 2. Addresses antivirus and updated definitions 3. Addresses operating system and software patches 4. Address change management issues. 5. Complete the on-line security and awareness training.</td>
<td>1. Determine how the system is to identify and authenticate each user. 2. Determine what logical and physical access controls should be in place. 3. Addresses operating system and software patches 4. Address change management issues. 5. Complete the on-line security and awareness training.</td>
<td></td>
</tr>
</tbody>
</table>
Official Use

Develop a security plan that addresses the following controls if the system is connected to systems that contain official and confidential data:

**Physical Controls**
1. Restrict physical access to IT computing resources that contain confidential data to those who require access to it.
2. Physically secure confidential data and do not leave it unattended on desks, open shelves and printers.
3. Lock documents that contain confidential information in storage rooms or drawers when not in use.

**Technical Controls**
1. Determine how the system is to identify and authenticate each user.
2. Determine what logical and physical access controls should be in place.
3. Perform routine scans and audits for security vulnerabilities.
4. Configure system to provide the least privilege level of access necessary to perform job function.

**Operational Controls**
1. Addresses documentation requirements
2. Addresses antivirus and updated definitions
3. Addresses operating system and software patches
4. Address change management issues.
5. Properly sanitize or shred discarded data.
6. Complete the on-line security and awareness training.
7. Develop a contingency and disaster recovery plan for each system.

Desktop

Department

Enterprise

Develop a security plan that addresses the following controls if the system is connected to systems that contain official and confidential data:

**Physical Controls**
1. Restrict physical access to IT computing resources that contain confidential data to those who require access to it.
2. Physically secure confidential data and do not leave it unattended on desks, open shelves and printers.
3. Lock documents that contain confidential information in storage rooms or drawers when not in use.

**Technical Controls**
1. Determine how the system is to identify and authenticate each user.
2. Determine what logical and physical access controls should be in place.
3. Perform routine scans and audits for security vulnerabilities.
4. Configure system to provide the least privilege level of access necessary to perform job function.

**Operational Controls**
1. Addresses documentation requirements
2. Addresses antivirus and updated definitions
3. Addresses operating system and software patches
4. Address change management issues.
5. Properly sanitize or shred discarded data.
6. Complete the on-line security and awareness training.
7. Develop a contingency and disaster recovery plan for each system.
Confidential

Develop a security plan that addresses the following controls if the system is connected to systems that contain official and confidential data:

Physical Controls
1. Restrict physical access to IT computing resources that contain confidential data to those who require access to it.
2. Physically secure confidential data and do not leave it unattended on desks, open shelves and printers.
3. Lock documents that contain confidential information in storage rooms or drawers when not in use.

Technical Controls
1. Determine how the system is to identify and authenticate each user.
2. Determine what logical and physical access controls should be in place.
3. Perform routine scans and audits for security vulnerabilities.
4. Configure system to provide the least privilege level of access necessary to perform job function.
5. Enable screen locking feature on systems that contain confidential information.
6. Enable auditing logs to trace the action of all users.
7. Audit accounts on systems that contain strictly confidential data.
8. Encrypt data in transit and in storage.

Operational Controls
1. Addresses documentation requirements
2. Addresses antivirus and updated definitions
3. Addresses operating system and software patches
4. Address change management issues.
5. Properly sanitize or shred discarded data.
6. Develop contingency and disaster recovery plans for each system.
7. Complete the on-line security and awareness training.

Desktop

Develop a security plan that addresses the following controls if the system is connected to systems that contain official and confidential data:

Physical Controls
1. Restrict physical access to IT computing resources that contain confidential data to those who require access to it.
2. Physically secure confidential data and do not leave it unattended on desks, open shelves and printers.
3. Lock documents that contain confidential information in storage rooms or drawers when not in use.

Technical Controls
1. Determine how the system is to identify and authenticate each user.
2. Determine what logical and physical access controls should be in place.
3. Perform routine scans and audits for security vulnerabilities.
4. Configure system to provide the least privilege level of access necessary to perform job function.
5. Enable screen locking feature on systems that contain confidential information.
6. Enable auditing logs to trace the action of all users.
7. Audit accounts on systems that contain strictly confidential data.
8. Encrypt data in transit and in storage.

Operational Controls
1. Addresses documentation requirements
2. Addresses antivirus and updated definitions
3. Addresses operating system and software patches
4. Address change management issues.
5. Properly sanitize or shred discarded data.
6. Develop contingency and disaster recovery plans for each system.
7. Complete the on-line security and awareness training.

Department

Develop a security plan that addresses the following controls if the system is connected to systems that contain official and confidential data:

Physical Controls
1. Restrict physical access to IT computing resources that contain confidential data to those who require access to it.
2. Physically secure confidential data and do not leave it unattended on desks, open shelves and printers.
3. Lock documents that contain confidential information in storage rooms or drawers when not in use.

Technical Controls
1. Determine how the system is to identify and authenticate each user.
2. Determine what logical and physical access controls should be in place.
3. Perform routine scans and audits for security vulnerabilities.
4. Configure system to provide the least privilege level of access necessary to perform job function.
5. Enable screen locking feature on systems that contain confidential information.
6. Enable auditing logs to trace the action of all users.
7. Audit accounts on systems that contain strictly confidential data.
8. Encrypt data in transit and in storage.

Operational Controls
1. Addresses documentation requirements
2. Addresses antivirus and updated definitions
3. Addresses operating system and software patches
4. Address change management issues.
5. Properly sanitize or shred discarded data.
6. Develop contingency and disaster recovery plans for each system.
7. Complete the on-line security and awareness training.
8. Determine how the system is to identify and authenticate each user.

Enterprise

Operational Controls
1. Addresses documentation requirements
2. Addresses antivirus and updated definitions
3. Addresses operating system and software patches
4. Address change management issues.
5. Properly sanitize or shred discarded data.
6. Develop contingency and disaster recovery plans for each system.
7. Complete the on-line security and awareness training.
8. Determine how the system is to identify and authenticate each user.

Physical Controls
1. Restrict physical access to IT computing resources that contain confidential data to those who require access to it.
2. Physically secure confidential data and do not leave it unattended on desks, open shelves and printers.
3. Lock documents that contain confidential information in storage rooms or drawers when not in use.

Technical Controls
1. Determine how the system is to identify and authenticate each user.
2. Determine what logical and physical access controls should be in place.
3. Perform routine scans and audits for security vulnerabilities.
4. Configure system to provide the least privilege level of access necessary to perform job function.
5. Enable screen locking feature on systems that contain confidential information.
6. Enable auditing logs to trace the action of all users.
7. Audit accounts on systems that contain strictly confidential data.
8. Encrypt data in transit and in storage.
Desktop
awareness training. 8. Determine how the
system is to identify and authenticate each
user. 9. Determine what logical and physical
access controls should be in place. 10. Perform routine scans and audits for
security vulnerabilities. 11. Configure system to provide the least
privilege level of access necessary to
perform job function.

Department
8. Determine how the system is to identify and
authenticate each user. 9. Determine what logical and physical access
controls should be in place. 10. Perform routine scans and audits for
security vulnerabilities. 11. Configure system to provide the least
privilege level of access necessary to perform job function.

Enterprise
authenticate each user. 9. Determine what logical and physical access
controls should be in place. 10. Perform routine scans and audits for security
vulnerabilities. 11. Configure system to provide the least
privilege level of access necessary to perform job function.

**SYSTEM DATA CLASSIFICATION SIGN-OFF**

1) I have classified my systems based on the GW Data Classification Policy and Matrix.

2) Out of compliance conditions with the GW Data Classification Policy and Matrix have been documented and a risk assessment completed.

<table>
<thead>
<tr>
<th>System Administrator Sign-off</th>
<th>System Owner Sign-off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td>___________________________</td>
<td>_______________________</td>
</tr>
<tr>
<td>Signature:</td>
<td>Signature:</td>
</tr>
<tr>
<td>___________________________</td>
<td>_______________________</td>
</tr>
<tr>
<td>Title:</td>
<td>Title:</td>
</tr>
<tr>
<td>___________________________</td>
<td>_______________________</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
<tr>
<td>___________________________</td>
<td>_______________________</td>
</tr>
</tbody>
</table>