**CYBER SECURITY INCIDENT REPORTING TEMPLATE**
APPENDIX A

| Contact Information | |
|---|---|
| **Individual's Name** | |
| **Agency Name** | |
| **E-Mail Address** | |
| **Phone Number** | |

**Statewide Cyber Security Incident Reporting Hotline:**

**208-332-1505**

*(Available 24x7. If no answer, leave message & responder will return your phone call promptly)*

| Description of Incident | |
|---|---|
| **Date / Time Incident Detected** | |
| **Date / Time Incident Occurred** | |
| **Type of Incident**<br>(Examples: Web defacement, virus, etc) | |
| **Method of Intrusion**<br>(Example: Vulnerability exploited, compromised account, etc) | |
| **Level of Unauthorized Access Attained**<br>(Example: root, administrator, user, etc) | |
| **Any Other Relevant Information**<br>(Attach log extracts as separate document/file) | |

| Affected System(s) | |
|---|---|
| **IP Address(es)** | |
| **Hostname(s)** | |
| **Purpose of System**<br>(Example: DNS server, router, e-mail server, application server, etc) | |
| **Operating System**<br>(Include version and patch levels) | |
| **Description of Protection In Place**<br>(Example: Agency firewall, intrusion detection system, anti-virus, etc) | |
| **Ports of Communication**<br>(Example: TCP port 21, UDP port 53, etc) | |
| **Physical Location of System (or Network)** | |
| **Attempted Attack Vectors**<br>(Describe the type of attacks attempted against the system and/or network, if known) | |

| Attack Source(s) | |
|---|---|
| **IP Address(es)** | |
| **Hostname(s)** | |
| **Ports of Communication (if known)**<br>(Example: TCP port 21, UDP port 53, etc) | |
| **Any Other Relevant Information** | |

| Damage Assessment (may be estimated) | |
|---|---|
| **Impact of attack on Agency operations and/or services** | |
| **Staff time to detect, handle, and recover from the incident** | |
| **Costs due to information loss, downtime, or other** | |
| **Current System (or Network) Status** | |