## Initial Impact Assessment Template

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [Organization] Internal Data Security Incident Alert | | | | **TLP:RED** |
| Alert Date and Time | | Month DD, 20xx, 12:00 a.m. / p.m. | | |
| Incident Name/Number | | [Descriptive name or numbered naming convention] | | |
| Type | [Ransomware, Malware Infection, Data Breach, DDoS, or other attack type] | | | |
| Incident Details | [Provide a summary (in less than 6 lines) of the incident impacts. Include, what happened, when it occurred, when and how it was discovered, and any additional high-level details appropriate for senior management notification. Consider using the 5 W’s and Impacts] | | | |
| Public Impacts | [Status of Public Website, Payment Processing, Public Data Systems, Public Safety Answering Point, SCADA Systems, or other public facing system] | | | |
| Internal Impacts | [Status of organization email, phone system, computer workstations, internal document and records storage, public safety, or other internal systems] | | | |
| Current Containment Activities | | | | |
| 1. [List major activities taken to contain impacts] | | | | |
| Planned Actions | | | | |
| 1. [List major actions planned to further contain and eradicate active threat] | | | | |
| Supporting Actions or External Assistance Requests | | | | |
| 1. [List any supporting actions or external requests needed to facilitate incident response activities] | | | | |
| Next Scheduled Update | | | Month dd, 20yy at 12:00 a.m./p.m. or as conditions warrant. | |