**INCIDENT RESPONSE REPORT**

|  |  |
| --- | --- |
| **ORGANIZATION NAME** | [BEC\_COMPANY] |
| **INCIDENT NAME** | [BEC\_INCIDENT] |

|  |  |  |
| --- | --- | --- |
| **INCIDENT OWNER** | **DATE COMPLETED** | **TICKET NUMBER** |
| [INCIDENT\_OWNER] | [COMPLETION\_DATE} | [BEC\_TICKET] |

INCIDENT SEVERITY

|  |  |  |
| --- | --- | --- |
| **X** | **LEVEL** | **ADDITIONAL COMMENTS REGARDING INCIDENT SEVERITY** |
| **[H]** | HIGH | [SEVERITY\_COMMENTS] |
| **[M]** | MEDIUM |
| **[L]** | LOW |
|  | OTHER |

INCIDENT TYPE

|  |  |  |  |
| --- | --- | --- | --- |
|  | Endpoint Compromise |  | Malware |
|  | Denial-of-service | **X** | Email Compromise |
|  | Sweeps, scans, or other reconnaissance |  | Theft |
|  | Phishing |  | Other (please describe) |
| **ADDITIONAL COMMENTS / “OTHER” DESCRIPTION** | | | |
| [ADDITIONAL\_COMMENTS] | | | |

INCIDENT TIMELINE

|  |  |
| --- | --- |
| **DATE AND TIME OF INCIDENT** | **DATE AND TIME OF DISCOVERY** |
| [COMPLETION\_DATE]  [INCIDENT\_TIME] | [COMPLETION\_DATE] [ALERT\_DISCOVERED] |
| **CLOSURE DATE** | **EXPLANATION FOR CLOSURE** (resolved, false positive, other) |
| [COMPLETION\_DATE] | Resolved |

INVESTIGATION AND RESPONSE TIMELINE

|  |  |  |  |
| --- | --- | --- | --- |
| **ACTION** | **TIME** | **OWNER** | **NOTES** |
| Incident Response Commencement | [ALERT\_DISCOVERED] | [INCIDENT\_OWNER] | Initial alert of compromise triggering the IR process |
| Secured User Account | [SECURED\_TIME] | [INCIDENT\_OWNER] | Reset Users Password with MFA Enforced  Revoked User Sessions  Pulled audit logs for user activity  Assisted user with new password and MFA set up |
| Incident Response Closure | [COMPLETED\_TIME] | [INCIDENT\_OWNER] | IR Procedure complete Notifying customer management of incident |

IMPACT OF INCIDENT

|  |  |
| --- | --- |
| **SYSTEMS AFFECTED** | N/A |
| **IMPACT ON OTHER INVOLVED PARTIES** | [OTHER\_PARTIES] |
| **ADDITIONAL DETAILS** | [ADDITIONAL\_DETAILS] |

SECURITY RECOMMENDATIONS

|  |
| --- |
| [SEC\_RECOMMEND] |