

# Safely Handling Malware Checklist

| Details of the Organization            |  |
|--|--|
| Organization Name:                     |  |
| Contact Number:                        |  |
| Website:                               |  |
| Address:                               |  |
| <i>Additional Contact Information:</i> |  |
|  |  |

| Details of the First Responder              |  |                               |  |
|---|--|-------------------------------|--|
| Date of the Incident:                       |  | Date Report Processing Began: |  |
| Name:                                       |  | Report Number:                |  |
| Job Title:                                  |  | Department:                   |  |
| Email Address:                              |  |                               |  |
| Phone Number and, If Applicable, Extension: |  |                               |  |
| <i>Small Description of the Incident:</i>   |  |                               |  |
| <i>Additional Details (If Any):</i>         |  |                               |  |

| Measures to Safely Handle Malware during Investigation   |                          |
|--|--------------------------|
| Actions  | Completed                |
| Whether a virtual machine or sandbox environment is used for handling malware  | <input type="checkbox"/> |
| Whether the virtual machine or sandbox environment is isolated from functional network systems   | <input type="checkbox"/> |
| Whether dedicated secure channels are used for transferring malware files  | <input type="checkbox"/> |
| Whether dedicated secure universal serial bus (USB) drives are used for transferring malware   | <input type="checkbox"/> |
| Whether malware files are zipped and password protected to avoid accidental execution  | <input type="checkbox"/> |
| Whether the identified malware file extensions are modified or added an invalid file extension to malware files to ensure no application is associated with it | <input type="checkbox"/> |
| Whether malware files are stored in an isolated storage facility   | <input type="checkbox"/> |
| Whether the malware files with invalid file extensions and the directory where malware files are stored from antivirus scans were excluded                     | <input type="checkbox"/> |
| Whether snapshots of the files are made to easily roll back to a non-infected state after completing the analysis  | <input type="checkbox"/> |
| Whether hashing is used to fingerprint the malware sample  | <input type="checkbox"/> |
| Whether the affected systems are contained within the constrained VLANs that use additional segmentation and network access controls                           | <input type="checkbox"/> |
| Whether robust application logging and auditing are implemented  | <input type="checkbox"/> |

---

**Incident Responder's Signature**

---

**Date**