KEFRI/F/ICT/08



**ICT Security Incident Report**

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Communication & Technology (ICT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Contact Information for this Incident** | | | |
| Name: |  | | |
| Title: |  | | |
| Department/Division/Eco-Region/Center |  | | |
| Mobile Phone: |  | | |
| Email address: |  | | |
| **2. Incident Description**. | | | |
| Provide a brief description: | | | |
| **3. Impact / Potential Impact** Check all of the following that apply to this incident. | | | |
| * Loss / Compromise of Data * Damage to Systems * System Downtime * Financial Loss * Other Organizations’ Systems Affected * Damage to the Integrity or Delivery of Critical Goods, Services or Information * Violation of legislation / regulation * Unknown at this time | | | |
| Provide a brief description: | | | |
| **4. Sensitivity of Data/Information Involved** Check all of the following that apply to this incident.   |  | | --- | | **Sensitivity of Data** | | | | |
| * Public * Internal Use Only | | * Restricted / Confidential (Privacy violation) * Unknown / Other – please describe: | |
| Provide a brief description of data that was compromised: | | | |
| **5. Who Else Has Been Notified?** | | | |
| Provide Person and Title: | | | |
| **6. What Steps Have Been Taken So Far?** Check all of the following that apply to this incident. | | | |
| * No action taken * System Disconnected from network * Updated virus definitions & scanned system | | | * Restored backup from tape * Log files examined (saved & secured) * Other – please describe: |
| Provide a brief description: | | | |
| **7. Incident Details** | | | |
| Date and Time the Incident was discovered: | |  | |
| Has the incident been resolved? | |  | |
| Physical location of affected system(s): | |  | |
| Number of sites affected by the incident: | |  | |
| Approximate number of systems affected by the incident: | |  | |
| Approximate number of users affected by the incident: | |  | |
| Are non-KEFRI systems, such a business partners, affected by the incident?  (Y or N – if Yes, please describe) | |  | |
| Please provide any additional information that you feel is important but has not been provided elsewhere on this form. | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision History** | | | |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Approval History** | | | |
| **Approver Name** | **Designation** | **Signature** | **Date** |
|  |  |  |  |
|  |  |  |  |

**Please submit this completed form to:**

ict@kefri.org