|  |  |  |
| --- | --- | --- |
| Report Type | Date | NIS Reportable Incident |
| First Report(no later than 72 hours after identifying incident) | Click here to enter a date. | Choose an item. |
| Interim Report(optional) | Click here to enter a date. |  |
| Final Report (no later than 72 hours after resolving incident) | Click here to enter a date. |  |

|  |
| --- |
| Service Provider Details |
| Organisation Name |  |
| Sector | Choose an item. |
| Contact Person |  |
| Role/Title |  |
| Phone |  | **Email** |  |
| Availability |  |
| Other Interested Parties |  |

|  |
| --- |
| Incident Details  |
| Description Time/date incident discoveredTime/date incident occurred Internal reference numberHigh level description of incident |  |
| Service(s) affected | What essential services were affected: |
| Nature & Impact | Duration |  |
| Number of Affected Users |  |
| Nature of Compromise (authenticity, integrity, availability, confidentiality of data or service) |  |
| Geographic Spread |  |
| Cross Border Impact |  |
| Data Loss/Breach |  |
| Material Damage  |  |
| Financial Loss |  |
| Reputational Damage |  |
| Risk to Health, Safety or possible loss of life |  |
| Root Cause (if known) | Please tick relevant box |
| System failure (e.g. software bug, flawed procedure, hardware failure, etc.) |  | Natural disaster (e.g. storm, earthquake, etc.) |  | Human error (e.g. mistake, negligence, etc.) |  |
| Malicious action(e.g. cyber-attack, vandalism, theft, software bug, DDoS attack, etc.) |  | 3rd party failure(e.g. power cut, internet outage, etc.) |  | Other(please provide further detail below) |  |
| Root Cause narrative: |
| Severity | Please tick relevant box |
| Major Impact |  |
| Moderate Impact |  |
| Minor Impact |  |
| Not Yet Known  |  |
| No Impact (report for information only) |  |

|  |
| --- |
| Current Situation |
| Investigation Status  | Choose an item. |
| Actions Taken to mitigate or contain |  |
| Expected Time to Resolve |  |
| Support Required from CSIRT | Choose an item.  |
| Please provide further information:  |
| Notifications Issued(Impacted Parties, Executive Management, Law Enforcement, Data Protection Commissioner)  |  |

|  |
| --- |
| Information Sharing |
| Full Incident Information (ICT assets affected, IoC’s, etc.) |  |
| Lessons Learned(e.g. vulnerabilities/weaknesses exposed, new threats identified, inadequate processes/controls, staff awareness training needs, success of business continuity and disaster recovery plans, etc.) |  |

Please email completed form to certreport@decc.gov.ie