	National Defence Défense Nationale		Back to the DID List

DATA ITEM DESCRIPTION - DESCRIPTION DE DONNÉES

1. TITLE – TITRE	2. IDENTIFICATION NUMBER - NUMÉRO D'IDENTIFICATION
INCIDENT RESPONSE PLAN	**DID 3.10.10**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

The purpose of the Incident Response Plan is to detail the processes and procedures for the incident response activity which covers preparation for containment, eradication and recovery, as well as post-incident activity. Military systems should have proper incident containment, eradication, recovery, and post-analysis depending on their mission criticality and the underlying threat related to the incident.
The detection and analysis phase is to be covered in the Continuous Monitoring Plan CDRL 3.10.9 where the detection and analysis procedures and tools are defined and set up.

4. APPROVAL DATE DATE D'APPROBATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE PREMIERE RESPONSABILITÉ (BPR)	6. GIDEP APPLICABLE D'ÉCHANGE DE DONNÉES PERTINENT
TBD	NWSO Technical Authority (TA)	N/A

7. APPLICATION / INTERRELATIONSHIP – APPLICATION / INTERDÉPENDANCE

CDRL 3.10.10 and SOW paragraph 3.10.10 refer.
This DID contains the format and content preparation instructions for the data generated under the Work tasks described in the NWS O&M SOW.

8. ORIGINATOR - AUTEUR	9. APPLICABLE FORMS - FORMULES PERTINENTES
NWSO TA	NIL

10. PREPARATION INSTRUCTIONS – INSTRUCTIONS SUR LA PRÉSENTATION DES DONNÉES

10.1 Source Document

10.1.1 NWS O&M SOW Section 3, paragraph 3.10.10
10.1.2 U.S. National Institute of Standards (NIST) SP 800-61 Rev. 2, Computer Security Incident Handling Guide (doi: SP800-61 Rev. 2)
10.1.3 Developing an Operational Technology and Information Technology Incident Response Plan, Public Safety Canada, 2020, ISBN: 978-0-660-35443-9

10.2 Content and Format

10.2.1 The Incident Response Plan must be prepared and delivered in Contractor format.

10.2.2 The Contractor must establish and implement a Incident Response Plan which must document the following:
- a. Includes consideration for:
  - i. Potential system function losses and their mission impacts from MCAAV report;
  - ii. Assessed risks like described in risk assessment reports; and
  - iii. Response constraints (E.g. technology, resources, time, laws and regulations, etc.).
- b. The plan must include the objectives, procedures, support tools and necessary resources to respond to incidents;
- c. The plan must include a Disaster Recovery Plan which includes containment, eradication and recovery objectives:
  - i. Objectives on the containment of the impacts of the system function losses must be defined;
  - ii. For the threat events identified during risk assessment associated with a persistent access, containment and eradication objectives must be defined; and

iii. Recovery objectives must be identified for each system function loss, considering the DND/CAF missions, operations and capabilities that the system function support. Objectives must be defined in terms of mission assurance metrics (E.g. time lapses, percentages, etc.).

d. Include a post-analysis procedure in which:
   i. Impacts caused by the incident are documented;
   ii. Risks of similar incident happening again are identified and managed;
   iii. Performance of the incident response procedures are measured against the objectives defined in c); and
   iv. Solutions for improving incident responses are defined when the observed performance does not meet the objectives.

10.2.3 Security categorization of the Incident Response Plan deliverable must be performed upon creation of the document, as the Incident Response Plan or certain portions could be Protected. Security labelling and marking, as well as handling, storage and transmission of the Incident Response Plan must be implemented in accordance with National Defence Security Orders and Directives. In addition to the Security Marking, which is placed in the header and footer of each page, a set of informative statements will be printed on the cover, or first page, of the document and in some cases also on the Verso Page (the back-side of the Title Page or Cover Page) as required.

10.2.4 The Contractor will be responsible for conducting change management as described below:

a. The Incident Response Plan must include a change history summary section which contains the following:
   i. A clear and unique version/revision identifier for each submission or resubmission of the Incident Response Plan;
   ii. Clear identification of revisions or amendments within the document from its previous submission; and
   iii. Rationale for the revisions and amendments.

b. All the above revisions/amendments must be clearly identified within the document by using suitable change tracking feature in the Office Management Software used to produce the document, e.g. "Track Changes" feature in Microsoft-Word®, side bars etc.

Page 2 of 2
December 2020