IT Security Incident Report to Management

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) 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:	KARTHIC kumAR·m
Title:	IT mANAGER
Program Office	
Work Phone:	
Mobile Phone:	8012922447
Email address:	karthi @ dignityindia ·com
Fax Number:	

2. Incident Description.

Provide a brief description:

* ERP Server down. (Cloud)

* Due to bandwidth & Storage issue

* Issue resolved from vendor end

* Process resumed

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:

* Down time for ERP users

4. Sensitivity of Data/Information Involved Check all of the following that apply to this incident.

Sensitivity of Data

Category	Description
Data Loss	N/A
Un Authorized Access	N/A
Invalid Password attempts	N/A
Virus Deduct	N/A
Power Issues	N/A
Software Corruption	N/A
Hardware Issues	N/A

☐ 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: MR. NAMASHIVAYAM

HVP – HR & ADMIN

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:	July 21, 2022
Has the incident been resolved?	Yes
Physical location of affected system(s):	N/A
Number of sites affected by the incident:	N/A
Approximate number of systems affected by the incident:	N/A
Approximate number of users affected by the incident:	All ERP users
Are non-Commonwealth systems, such a business partners, affected by the incident? (Y or N – if Yes, please describe)	N/A
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	N/A