Introduction

This update covers tracking for IT incident management items supplemental to technical updates from the incident remediation team.
The owner of the overall incident remediation is <insert unit owner>.

This update is confidential and privileged, shared only with <name & role>, <name & role> and cannot be shared further.

Ownership inquiries: contact <name & role>
Responsible for document updates:
Section 1 below ("add comments" section): <name & role>
Sections 2-4 below (main report): <name & role>

There are 4 sections:

1. Update/Comment Log: section for interim updates by participants.
2. Action Log & 2A. Action Log Update Tracking
3. Timeline Log & 3A. Timeline Log Update Tracking
4. Key Participants

1. Update/Comment Log (interim updates)

	Name	Date		Update(s)	File updates
	e.g. Name	*Nov-11*	*Comment to be added here*		*Added 2C below*
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

2. Action Log

	Focus Areas	Owner	Status	Updates	Outputs
A1	Technical impact inventory (which will benefit PII impact assessment). This includes data gathering for impacted inventory as well as faculty, staff, researchers and others (including inactive accounts/users)* More detailed research impact noted in section A2 below.	Name, Date If an owner is updated keep the previous owner on record.	In progress	**This section is centered around the completion of the Excel file inventory** Date: complete an asset/inventory spreadsheet indicating server, workstation, account, service, etc. .. For each asset indicate operational, teaching, research impact with a “Yes, No, Maybe” indicator.	Excel template
A2	Research specific impact assessment	Name, Date If an owner is updated keep the previous owner on record.	In progress	**This section is specific to research impact** Date: Based on above activity: article all research in the unit and clearly identify what is not impacted to ascertain next steps. Identify key, impacted research partnerships for further assessment Date: research items which require more identifiable details;	Excel template
B	Impacted client notification activities	Name, Date If an owner is updated keep the previous owner on record.	In progress	**This section covers impacted client interactions”* *Completed activities:* - Active users forced to change passwords and SSH keys - Unit--wide email circulated (ascertain feedback) - Consulted with a specific affected, targeted user - Consulted with affected counterparts *Pending activities:* - Assess next steps based on full asset inventory	Email updates Excel tracking

				Record all interactions and activities: Date: <interaction & activities>	
C	c. Incident Management communication and escalation *(Also see section 3 below – timelines and activities)*	Name, Date If an owner is updated keep the previous owner on record.	In progress	**This section covers overall IM engagement activities** *Activities:* - Escalation to the Chair by <name, role> - Escalation to the Dean by <name, role> - Escalation to VPRI by <name, role> - Escalation to FIPP by <name, role> - Escalation to legal counsel by <name, role> - Escalation to institutional Incident Management team by <name, role> *Pending activities:* - Escalation to authorities by <name, role> *Record all interactions, activities and actions*: Date: <interaction and activity> Action 1: Action 2:	Email updates and meeting minutes to be provided

2A. Action Log Update Tracking
Updated/<Name>: <date & time>
Updated/<Name>: <date & time>
…

3. Timeline Tracking

Date MM-DD	Description	Comments/source of update
	Start of incident (to be confirmed through analysis and technical validation)	<name & role>
	Compromised account, services, machines issue reported	<name & role>
	Containment	<name & role>
	Issue reported to <name & role> with an email summary	<name & role>
	Escalation	<name & role>
	Remediation	<name & role>

3A. Incident manager tracking update: Timeline Log Update Tracking
Updated/<Name>: <date & time>
Updated/<Name>: <date & time>
…

4. Key Participants

**others to be added*

Role	Name	Active and/or Informed
IT Lead		A
IT Director		A
CISO		A
IS Director		A
FOIL		A, I
Dean		I
Vice-Dean		A, I
CAO		A, I
U of T members	Incident Management, FIPP, Legal	A, I