# Mission Continuity Program (MCP)
# FY22 Tabletop Exercise Scenario

# Introduction

- Time of year:  Winter 2022
- Time of day:  9:00 AM
- Weather: Cold but clear

- As a part of this exercise, please inform the Mission Continuity Program by April 30, 2022 of your organization's **most critical technology systems** (2-4 total) in rank order that are needed in order to continue your critical operations.

# Day One, 9 AM

- You are informed that a Penn School or Center your organization works closely/partners with (choose one) has been attacked with ransomware.  Your organizational leadership (Dean, Vice President, Executive Director) immediately calls an emergency meeting for later this morning to discuss how to prepare your organization in the event the same thing happens to you.

❑Who needs to attend the meeting?  Do you have a Contact Group in Shadow-Planner for the appropriate group, for example an Incident Management team (IMT)?  Does the team include your Local Support Provider (LSP) or other rep from IT  support?

# Day One, 11 AM

- The meeting convenes.  Several people are on vacation and therefore unable to participate.  Choose 1-3 people from among your TTX attendees who will not participate;  include a senior leader among them. They may remain in the room to listen during the TTX but may not contribute.

❑Do you have a Loss of Human Resources plan to deal with the absence of key people?

# Day One, 11 AM continued

- The first discussion item is to determine your organization's most critical services which would need to continue or resume in the event of a ransomware attack.

q Can you determine what data and applications your organization needs in order to continue your critical services, so you know what needs to be backed up and restored in the event of a ransomware attack?

q Is your Business Impact Analysis (BIA) information in Shadow-Planner up-to-date with your organization's most critical processes and functions? A report of this information should be circulated to the group and discussed to ensure it is complete and current.

# Day One, meeting continues

- The discussion turns to the use of backups as protection in the event of possible ransomware attacks.

❑Do you have a Loss of Technology plan(s) in Shadow-Planner? Does it include information about taking backups?

❑Do you have backups in place for critical computer systems and applications?

❑According to your LSP or IT Director, what would be the process and how long would it take to restore critical systems and applications using backups? Is this process reflected in your Loss of Technology plan(s)?

# Day One, meeting continues

- Your organization's leadership has also heard of ransomware that exfiltrates or removes sensitive files to the attacker.  They ask the following questions:

❑Does your organization have an inventory of all Moderate/High risk data as referenced in Penn's Data Risk Classification schema, and on which systems it is located?

❑Do you have a plan to routinely delete data that is no longer needed?

# Day One, meeting continues (optional discussion)

- The discussion proceeds to other protections in place to respond to the threat of ransomware.  Leadership at the meeting asks your LSP or IT Director the following questions.

- ❑What firewalls are in place?
- ❑On what accounts do you have two-factor authentication enabled?
- ❑How often are patches applied to critical systems and applications?
- ❑Do you have logging to detect intrusions on critical systems and applications?
- ❑Do you do regular Disaster Recovery (DR) exercises?
- ❑Do you have a Loss of Technology plan in Shadow-Planner with steps to take in the event of a ransomware attack?

# Day Two, 9 AM

- Pick one of the following communication tools (preferably the one your organization uses the most). You arrive at work to discover this tool is down due to a ransomware attack on the vendor.
  - Zoom, MS Teams, Slack, Blue Jeans, Penn+Box, OneDrive, Sharepoint
- You contact the Office of Information Security for guidance and they tell you to work with ISC to understand what data are affected.

❑What critical processes and functions are affected by this vendor? Are these processes and functions listed in your BIA?

❑What alternatives/workarounds do you have in your MC plans to deal with a loss of this vendor or loss of access to this collaboration tool/data?

# Day Three, 9 AM

- You arrive at work to discover a ransomware attack on your organization's computers.  When you try to access your computer, you can only get a pop-up message saying your files are unavailable unless you pay a large amount in bitcoin to a certain account. You discover that certain University-wide systems, such as BEN Financials and Pennant, have been compromised by the attack.
- You call your LSP or IT Director.  You also contact Penn's Office of Information Security for guidance in dealing with the attack.  Your organization starts to execute your Loss of Technology plan.

❑Does your plan include communications with the appropriate people?  Do you have access to an out-of-band communications tool or phone/text?

❑Are you prepared to start the process of restoring critical processes and functions based on the preparation you did earlier?

❑What workarounds do you have in place so your organization's staff can continue to deliver on your core mission while this is happening?  Are these workarounds listed in your BC plans?

# Day Four, 4 PM

- You are informed that University leadership have decided Penn will not pay the ransom.  Your organization begins the process of recovering from the attack.

❑What critical services have been impacted as a result of this incident?

❑What are the potential impacts to University business (for example, financial or reputational)?

❑What is the estimated timeframe for full recovery?

❑What critical decisions need to be made, if any?

# Day Five, 11 AM

- As a result of the ransomware attack, your organization decides that you need to order new laptop computers.  Your LSP contacts the vendor, who says there is a 6-month wait time due to supply chain issues.

❑Do you have a Loss of Third-Party Vendor/Partner plan in Shadow-Planner to deal with this?

❑What is your alternative plan/workaround for not being able to obtain new computers?

# One month later

- University-wide most-used applications, such as BEN Financials and Pennant, have been recovered.  However, other, more local systems remain unavailable.

- What are your manual fallback procedures and are they documented in Shadow-Planner Action Plans?
- How have you been able to continue your portion of the University's mission under these circumstances, including work such as paying bills, running reports, booking facilities and classrooms, delivering instruction and managing research grants?

# Mission Continuity Planning

- Were our plans adequate for this type of loss and disruption to normal operations?
- Are we able to continue operations without major impact to our constituents?
- Post-exercise analysis:
  - Do we need to modify our Mission Continuity plans, DR plans, or BIA?
  - What was missing in the steps we took during the scenario?
  - What would we do differently?
  - Please review your Recovery Time Objectives (RTOs) and Achievable Recovery Times (ARTs) as listed in your BIA.  Do any of these need to be adjusted, based on the experience of this scenario?
  - Are we comfortable with our response and ability to recover?
  - Did we succeed in protecting Penn assets?