This document describes the incident response procedures for regular operational issues that occur in the secure research project repository. Note: Security incidents should be handled following the security incident response procedures.

Overview:

Expectations:

End users are expected to have reasonable expectations for support in the NIST environment. Standard support is offered from 8:00 am – 5:00 pm during normal business days. After hours support is handled slightly differently than standard support.

Standard support expectations:

End users are expected to follow standard ITS/CTS procedures for handling tickets after having consulted with their local IT support staff. ITS staff will respond to tickets based on the priority assigned to the ticket and based on the current workload of other incidents.

After hours support expectations:

After hours support is provided on an on-call basis. FSU does not have ITS staff working a normal shift after hours. The use of on-call personnel may incur an additional cost to FSU. End users are expected to limit the use of after hours support to critical issues which cannot reasonably wait until standard support is available. After hours incidents should only be opened after the end user has exhausted any reasonable attempts at resolving the incident using local unit IT support staff and working around the incident if possible. For example, if the end user's NIST workstation is not working, has the end user tried to use another NIST workstation to perform the same function?

Roles and Responsibilities of key stakeholders/provider groups:

ISPO/Research Data Security Specialist (RDSS)

- Responsible for monitoring incidents and assisting with getting any incidents resolved
- May escalate and route incident tickets as deemed appropriate

Research Principal Investigators (PIs) and other staff who utilize Controlled Unclassified Information

- Should contact the appropriate staff to get their incidents resolved. See the procedures below.

Local unit IT Support staff –

- (in some cases) are responsible for maintaining the local area network in the office and ensuring that workstations and laptops have network connectivity as appropriate.

- Responsible for ensuring that initial basic troubleshooting steps regarding on premise workstations and VPN/RDP laptops and workstations has been done. For example, power cords are connected securely, network cables are connected securely, network availability has been confirmed, etc.

Computing Technology Support – (provider group ITS-NIST)

- Responsible for configuring and supporting on premise desktops
- Responsible for configuring and supporting VPN/RDP laptops and workstations.

ITS MEAS team – (provider group ITS-MSTS)

- Responsible for configuring and supporting Windows Servers in the AWS Management VPC.
- Responsible for configuring and maintaining the AWS environment.
- Responsible for configuring and supporting Windows hosts in the project secure areas in AWS.

ITS LEAS team – (provider group ITS-UNIX)

- Responsible for configuring and supporting Linux hosts in the project secure areas in AWS
- Responsible for configuring and supporting Linux hosts in the AWS management VPC

NCT CORE – (provider group ITS-CORE Networking)

- Responsible for configuring access from the FSU environment to the AWS environment
- Responsible for configuring and supporting the firewalls in the AWS environment
- Responsible for configuring and supporting on premise firewalls providing VPN connectivity to the AWS environment
- (in some cases) are responsible for maintaining the local area network in the office and ensuring that VPN/RDP workstations have network connectivity.

Incident Response Procedure:

1. The end user should initially contact his/her local unit IT support.
2. Local unit IT support should perform initial triage of the incident to determine if it can be resolved locally, for example, confirming power cords are connected securely, network cables are connected securely, network availability has been confirmed, etc.
3. If the local unit IT support person cannot resolve the issue, a ticket should be opened in the ITS Service Center or by calling 644-HELP. At a minimum, the ticket should identify the following:
    - Customer Information:
        - Name
    - Problem Information
        - Summary of the problem
        - Detailed description of the problem. If you have an alternate phone number, include it in the description so that the technician can call you if needed.

- Case Information
  - Enter ITS-NIST in the Provider Group
  - Specialty Type NIST
  - Enter the Case Priority (see https://servicecenter.fsu.edu/sites/g/files/upcbnu506/files/guidelines/ITS%20Response%20Time%20General%20Guidelines.pdf for the FSU Service Center Response Time Guidelines).

4. If the local unit IT support has confirmed that the ticket needs to be assigned to another team, the ticket can then be assigned to the appropriate provider group for that team. Do not do this until the case has been initially created and assigned to the ITS-NIST provider group. Assigning it initially to the ITS-NIST provider group will ensure that a notice will go out to the NIST provider group who will monitor this ticket to ensure it is being responded to in a timely manner.
5. If you require after hours support, call 644-HELP. Note: the after hours operator does not have the ability to diagnose or resolve any issues. The after hours operator can only call the on call support person. If the local unit IT support person has triaged the issue and identified that this ticket should be routed to a specific provider group, ask the operator to call the on call person for that specific provider group. If you have not identified a specific provider group to route the ticket to, ask the operator to call the on call person for the ITS-CTS provider group. Provide the operator with the ticket number you created in step 4. Also provide a phone number where you can be reached.
6. Monitor your email. You may or may not get a callback. If the assigned technician is able to diagnose your issue based on the information you provided in the ticket, he will do so and update or close your ticket as appropriate. You will get an email response from the service center system.

Additional Incident Response information:

Questions the service desk will ask when called during normal business hours:

- Here are the initial list of questions I provided to the Service Desk so they can start gathering information related to the service ticket.
  - The name of the service – NIST (as you have currently entered. I may want to change this to NEST in the future, but for now leave it at NIST)
  - Brief description of the service - the description you have is fine
  - The Service Category (for CRM/FM) – NIST.
  - Any FAQs/web pages we have about the service - https://www.research.fsu.edu/research-compliance/research-data-security/
  - What troubleshooting the Service Desk needs to do (if any) – basic troubleshooting
  - Any information the Service Desk needs to gather before routing the case – Name of user and contact details (fsu email, phone, location), detailed description of the problem, project associated with NIST. Note: ITS Service desk will not be able to reset passwords in the NIST environment.
- Other questions to ask:
  - Ask if the user can connect to the NIST environment?

- Ask if the user is trying to connect to a windows machine or a Linux machine?
- Ask if the user receives any error messages? If so, what are the details of the error messages?
- Ask if the user has received a device enrollment email from DUO Security.
- Ask if the user has successfully installed the DUO app.
- Ask if the user has successfully enrolled a mobile phone as an MFA device in the DUO app. In the DUO app, a registered device should have an entry named Florida State University – NIST.
- Ask if the user is aware of any other NEST users that have successfully connected to the Global Protect VPN with MFA.
- Where the ticket will be routed (in CRM) – to the NIST group

Membership in the ITS-NIST Provider group should be:

Michael Boll
Brian Rue