PennState
New Kensington

Incident and Disaster Tolerance/Response Procedure

Procedure Number: PSU-NK-ITS-013
Date: September 28, 2017
Page Count: 5

Purpose:

To provide campus faculty and staff with an overview of campus policies and guidance in responding to computing/networking security compromises, virus infected systems, and events that render one or more computer or network systems inoperable. This procedure outlines how NK ITS Department personnel and the Office of Information Security (OIS) will respond in the event of a system compromise or disaster within or on campus property.

Scope:

Incident response applies to the actions taken at all levels within Penn State University when a user's computer or any server is compromised for one or more of the following reasons:

- Compromise by brute-force attacks from within or outside the campus,
- Downloading of any virus that threatens campus communications and computing services,
- Connecting any non-patched or compromised system to the campus hardwired or wireless data network,
- Participating in any computing practices that are unlawful or contrary to campus and/or University computing policies
- Participating in any computing activities that prevent or have the potential to prevent others from carrying out the campus's academic and administrative missions.
- Incident response also applies to any reported or discovered illegal activities on any computer used on University premises, where illegal activities are defined by University policies and laws established by local, state, or federal governments.

Definitions:

Device – A computer, electronic tool or communication apparatus with the ability to connect to a data or communication network.

NK ITS Department – The department that oversees IT resources at Penn State New Kensington to include the System Administrator, IT Specialist and IT Director

New Kensington Data Network – The technology infrastructure, hardware, and software installed at the campus which is used to facilitate the flow of digital information between (but not limited to) computers, printers, servers, mobile devices, the Internet, etc. This includes both the wired and wireless networks at Penn State New Kensington.

Personally Identifiable Information (PII) – is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. PII data is commonly exploited by criminals to steal an individuals' identity. The combination of a name and the following sensitive information are common examples; Social Security Numbers (SSNs), credit card numbers, Driver's License numbers, passport numbers, Personally Identifiable Health Information (PHI), salary and tax information related to individuals, details of University budgets, tenure or promotion information, staff employee review information, password or other system access control information, human subject information, admission and financial aid information and donor information.

Office of Information Security (OIS) - a group of individuals that are part of Penn State Information Technology Services (ITS) that is responsible for protecting the Penn State community from threats to our IT resources.

Disaster tolerance - applies to actions taken by the campus, a department, and users to ensure that computing operations and network services are maintained, or, at worst case, gracefully degraded and terminated.

Disaster Recovery - are those actions taken by the campus, departments, and users to recover from events that render computing operations and network services inoperable. Events that initiate actions to maintain or restore computing operations and network services include but are not limited to momentary/long-term power outages, hardware failures, fire, natural disasters, and malicious attacks that render servers or systems inoperable/degraded.

Procedure:

Incident Response

Any device found or suspected of violating any campus or University policy focusing on ensuring secure and safe communications and computing will be summarily and immediately disconnected from the New Kensington Data Network.

Users will be notified as quickly as possible of such action once NK ITS Department personnel or the Office of Information Security (OIS) personnel are satisfied that a real or potential threat to other users or the Internet in general has been mitigated. Individuals at any level (users, technical contact, campus security, and University security) have the obligation to report potential computer operational activities that may detract or prevent normal computing activities.

Any question relating to the scope of this policy may be directed to the Director of Information Technology.

Disaster Tolerance

Disaster Tolerance is a result of planned actions, policies, hardware deployments, and any other efforts aimed at preventing limited to momentary/long-term power outages, hardware failures, fire or natural disasters from causing long-term disruptions of campus academic or administrative activities. NK ITS Department assumes the responsibility for disaster tolerance in networking operations throughout campus-maintained telecommunications closets. NK ITS Department is also responsible for these activities as they relate to maintenance and operations of core campus servers (e.g., domain controller, file, print, etc.) and departmental servers maintained by NK ITS Department.

In an effort to achieve Disaster Tolerance within the aforementioned operations and services, NK ITS Department has implemented the following procedures:

- Maintain quick response service contracts for critical equipment
- Provide and maintain Uninterruptible Power Supplies (UPS') for network equipment deployed in Telecommunications Closets maintained by the campus
- Provide and maintain UPS' for all core campus servers maintained by NK ITS Department
- Provide and maintain at least one week of data backup for core campus servers maintained by NK ITS Department

Information Assurance

The following efforts will be made to curtail the loss of sensitive institutional data such as Personally Identifiable Information (PII) and non-public University data and to ensure the confidentiality, availability, and integrity of the data. These efforts are required to comply with federal, state and University regulations and policy to assure due-care is taken to protect the University against monetary and reputational loss in the event of a data compromise.

- Scan all high-risk University computer systems for PII and assure the removal or adequate protection of data in line with University policy and guidelines.
- Encrypt the contents of computer storage devices to ensure the integrity and security of University data while at rest.
- Conduct security awareness training to educate University employees of best computer security practices.
- Ensure University computer systems are maintained within University policy and best security practices.

Disaster Recovery

Disaster Recovery encompasses all those activities and steps necessary to restore personnel and systems' services that have been interrupted by an unforeseen event(s) that may include but is not limited to: momentary/long-term power outages, hardware failures, fire, natural disasters, and malicious attacks that render servers or systems inoperable/degraded. It includes making plans to relocate personnel in order to effectively reconstitute personnel and systems' services along with academic and administrative services.

Therefore, as soon as conceivably possible and approved by appropriate University or other authority, NK ITS Department personnel will enter building telecommunications closets for the purpose of assessing damage and serviceability of network hardware and core servers affected by a disaster. All equipment will be inventoried and categorized according to its serviceability. Steps will immediately be taken to procure and receive replacements for unserviceable equipment.

In the event that offices and equipment used daily by NK ITS Department are rendered uninhabitable, personnel will report to the Emergency Operations Center (EOC) as designated by the Chancellor. Replacement computing assets will be made available through emergency local purchases and dispersed storage of backup computing devices. The Director of Information Technology will work with the campus Financial Officer to establish emergency procurement procedures.

In the event of a minor disaster such as a long-term electrical power outage, The Director of Information Technology will work with the Business Service Director and the Office of Physical Plant (OPP) to have power generation equipment installed to restore critical networking services. The process to restore critical networking services can only begin after the Business Service Director or the Office of Physical Plant (OPP) have deemed the building safe for inhabitance.

Reconstitution of networking/telecommunication operations and computing services will receive the highest priority. Initially, only that equipment and tools that are absolutely required to support reestablishment of reliable/sustainable services will be procured under the aforementioned emergency procurement process.

Departments are responsible for establishing and implementing Disaster Recovery policies and procedures that will enable them to reconstitute operations and continue their academic and administrative missions.

Incident Response Enforcement

The Office of Information Security (OIS) and NK ITS Department personnel have the right and responsibility to identify and take immediate action to curtail any computing operation that violates University Policies. They have the right and responsibility to intentionally or randomly scan any systems on the New Kensington Data Network. Furthermore, they have the right and obligation to summarily curtail a system's computing activities that disrupt or are suspected of negatively impacting secure computing activities on the University data network and beyond.

Illicit and illegal activities are forbidden on the campus and University networks. Illicit activities are those which are expressly prohibited by department, University and/or campus policies and are illegal as defined by local, state, or federal laws; they include but are not limited to operating business for personal gains and use of computing resources for other than University business. It is the responsibility of a department head and the Director of Information Technology to ensure that individuals within their departments abstain from such practices. Should someone outside or within the department report such activities to a department head or NK ITS Department personnel, it is the responsibility of the department head or the Director of Information Technology to advise the offending party of the offense and to ensure that all remnants of such activities are removed immediately from the New Kensington Data Network and the computer or server on which it resides. Questions concerning illicit activities may be directed to the campus Director of Information Technology or the Office of Information Security (security@psu.edu).

Illegal activities are those that are contrary to local, state, or federal laws. Anyone aware of such activities must immediately contact the Director of Information Technology and the Office of Information Security (OIS). No further actions are to be taken at the department level until either the Director of Information Technology or the Office of Information Security (OIS) notifies the department head or NK ITS Department personnel. No one in a department is to discuss their knowledge or suspicion of illegal activities with individuals suspected of participating in such activities; this is ultimately the responsibility of the Office of Information Security (OIS).

Any faculty or staff member has the responsibility to identify and take immediate action to curtail any computing operation that violates departmental, campus or University Policies. At the department level and other than prescribed above, faculty, staff and students are explicitly prohibited from scanning systems on the New Kensington Data Network or University’s data backbone. Faculty, staff or students that have had a compromised or suspected compromised system identified are obligated to disclose the issue to NK ITS Department and work with them to remediate the issue prior to reconnecting the system to the New Kensington Data Network or University's data backbone.

Prior to restoring network access, systems must be validated as having been patched with the latest OS, updated and cleansed of any virus-laden or disruptive software.

Procedure History:

September 13, 2019 – PII scanning updated to reflect only high-risk systems
September 28, 2017 – Procedure created based off previous campus policy.