Incident and Disaster Tolerance/Response Policy  
COE–IDTR–01

1.0 Purpose
To provide College faculty and staff with an overview of the College’s policies and guidance in responding to computing/networking security compromises, virus infected systems, and events that render one or more network closets inoperable. This policy is intended to provide all users of College-based personal computers, servers, and networking hardware with information pertaining to how department Technical Contacts, ECS personnel, and the University Security Operation Services are expected to respond in the event of a system compromise or disaster within a College-operated network closet.

2.0 Scope
2.1 Incident Response:
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 College,
- Downloading of any virus that threatens continuous College communications and computing services,
- Connecting any non-patched or compromised system to the College’s hardwired or wireless network,
- Participating in any computing practices that are unlawful, against College or University computing policies
- Participating in any computing activities that prevent or have the potential to prevent others from carrying out the College’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.

2.2 Disaster Tolerance/Recovery:
Disaster Tolerance and Recovery are two distinctly different issues. Disaster Tolerance applies to actions taken by the College, a department, and users to insure that computing operations and network services are maintained or at worst case gracefully degraded and terminated. Disaster Recovery are those actions taken by the College, 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.

All College departments, Centers, and operational units are responsible for developing and implementing Disaster Tolerance/Recovery plans.

3.0 Policy
3.1 Incident Response:
Any desktop, laptop, workstation, server or other network capable device found or suspected of violating any College or University policy focusing on ensuring secure and safe communications and computing will summarily and immediately disconnected from the College of Engineering’s and University’s data backbone.

Users will be notified as quickly as possible of such action once ECS or University Security 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, College Security, and University Security) have the obligation to report any real or potential computer operational activities that may detract from normal computing activities.
All systems showing any evidence of malware or other compromise must be fully scanned for the presence of Personally Identifiable Information (PII). PII data is defined in the College’s Data Classification Standards and Security Requirements Policy. Any instance of PII data must be immediately reported to ECS and clearance must be given by ECS before any alteration to the disk is allowed. Upon clearance the system must undergo a complete system reinstall unless overwhelming evidence is presented to show that a rebuild for the system is technically arduous and further that the system can satisfactorily be cleaned of malware and/or otherwise secured without a complete rebuild.

Any question relating to the scope of this policy may be directed to ECS at support@engr.psu.edu.

3.2 Disaster Tolerance/Recovery:

3.2.1 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 College academic or administrative activities. ECS assumes the responsibility for Disaster Tolerance in networking operations throughout College-maintained Telecommunications Closets. ECS is also responsible for these activities as they relate to maintenance and operations of core College servers (e.g., email, web, data, etc.) and departmental servers maintained by ECS personnel.

In an effort to achieve Disaster Tolerance within the aforementioned operations and services, ECS has implemented the following procedures:
- Maintain spare components for critical networking hardware operations
- Maintain spare components for critical servers
- Provide and maintain Uninterruptible Power Supplies (UPS’) for network equipment deployed in Telecommunications Closets maintained by the College
- Provide and maintain UPS’ for all core College servers and departmental servers maintained by ECS
- Mirror College emails servers and deploy them in a secondary Telecommunications Closet so that they can assume email services in the event of a primary email cluster failure
- Provide and maintain at least two (2) months of data backup for core College and departmental servers maintained by ECS

3.2.2 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 are not limited to momentary/long-term power outages, hardware failures, fire, natural disasters, and malicious attacks that render servers or systems inoperable/degraded. It necessarily includes making plans to relocate personnel in order to effectively reconstitute personnel and systems’ services along with academic and administrative services.

It is neither economical nor practical to maintain 100% redundant hardware in preparation for any and all potential disasters. Therefore, as soon as conceivably possible and approved by appropriate University or other authority, ECS personnel will enter building Telecommunications Closets for the purpose of assessing damage and serviceability of network hardware and core/departmental server 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 ECS’ networking, computing and training personnel are rendered uninhabitable, personnel will report to the Design Groups facilities. Office or laboratory lab space will be made available to displaced personnel based on a separate agreement made by the Facility’s Manager, ECS’ Director and the College’s Associate Dean for Administration and Planning. Replacement computing assets will be made available through emergency local purchases. The ECS Director will work with the College’s Financial Officer to establish emergency procurement procedures.

In the event of a minor disaster such as a long-term electrical power outage, ECS’ Director will work with the College’s Facilities Coordinator and the Office of Physical Plant (OPP) to have power generation equipment installed to restore critical networking services. Naturally, this process assumes that a building remains serviceable and is approved for use by OPP or the appropriate authorities.
Reconstitution of networking 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.

4.0 Incident Response Enforcement
University Security Operations 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 University’s backbone. 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 University or beyond.

College Security Operations personnel have the right and responsibility to identify and take immediate action to curtail any computing operation that violates College or University Policies. They have the right and responsibility to intentionally or randomly scan any systems on the College’s 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 College, University or beyond.

Departmental Technical Contact personnel have the right and responsibility to identify and take immediate action to curtail any computing operation that violates departmental, College or University Policies. They have the right and responsibility to intentionally or randomly scan any systems on within a department’s computing resources. 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 College, University or beyond.

Illicit and illegal activities are forbidden on the College and University networks. Illicit activities are those which are expressly prohibited by Department, University and/or College policies and are not 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 their departmental Technical Contacts 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 Technical Contact, it is the Technical Contact’s responsibility to advise the offending party of the offence and to ensure that all remnants of such activities are removed immediately from the College’s network and the computer or server on which it resides. Questions concerning illicit activities may be directed to the College’s and University’s Security Officers at security@engr.psu.edu and security@psu.edu.

Illegal activities are those that are contrary to local, state, or federal laws. Anyone becoming aware of such activities must immediately contact the College’s and University’s Security Officers at security@engr.psu.edu and security@psu.edu. No further actions are to be taken at the department level until and when either the College or University Security Officer notifies the department head or Technical Contact. 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 University’s Security Officer.

Any faculty or staff member has responsibility to identify and take immediate action to curtail any computing operation that violates departmental, College or University Policies. At the department level and other than prescribed above, faculty, staff and students are explicitly prohibited from scanning system on the College’s network or University’s backbone. Faculty, staff or students that have had a compromised or suspected compromised system identified are obligated to report this to their Technical Contact. In cases where the a department Technical Contact is unavailable, individuals may contact the College’s Associate Director for Communication and Computing for assistance in system repair; this individual may be contacted by emailing Support@engr.psu.edu or by calling 3-3856.

Systems must be validated as having been patched with the latest OS updated and cleansed of any virus-laden or disruptive software.

6.0 Revision History
Last updated: 12/17/2009