TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.90 – **IT Event Management / Response (EM)**

POLICY STATEMENT: TTUHSC El Paso Information Technology Department shall ensure that department personnel work towards the overall mission of providing superior customer service and promoting a healthy, safe, cooperative work environment by adhering and complying with professional and ethical standards of conduct both internally and externally.

REASON FOR POLICY: The purpose of the Event Management/Response policy is to provide guidance and establish a standardized framework for remediating IT events that require more concentrated efforts to resolve, in a collaborative and expedient manner. Procedures and guidelines are to be followed to promote positive, professional, team-focused behaviors that lead to successful resolution of IT events using processes most conducive to event management. This policy is based on guidelines to promote Internal and External Communication, Intradepartmental collaboration and Improved adherence to processes and workflows necessary for successful event management/resolution.

WHAT IS COVERED IN THIS POLICY?: The procedures and guidelines outlined in this policy are supported and enforced by the office of the CIO. Included in this document are procedures and expectations for Event Response Team (ERT) and IT staff pertaining to receiving requests that are categorized as events and require response and/or remediation, communication workflows for internal and external dissemination of information, and expected behaviors and actions of the ERT.

WHO SHOULD READ THIS POLICY?: IT personnel that are classified as having an exempt title classification are expected to read and adhere to this policy as they will be eligible to serve on the ERT team after hours. Non-exempt employees must read and comply with this policy as during regular business hours, event response staff may also include non-exempt personnel.

WHAT HAPPENS IF I VIOLATE THIS POLICY?: Any person(s) violating TTUHSC El Paso Information Technology policies are subject to disciplinary action outlined in HSCEP ITP 56.50 Sanctions Policy1 and HR Policy HSCEP OP 70.31 Employee Conduct, Coaching, Corrective Action and Separation from Employment.

POLICY/PROCEDURE:

DEFINITIONS

- IT Event – an Information Technology related occurrence that is of importance and impactful to the operations of a department, end user, or institution. Please see the event matrix to determine levels of severity.
- Collaboration – the act or process of collaborating, to work with one another, cooperate, in a professional and productive manner; a cooperative agreement of two or more parties to work jointly towards a common goal.
- Event Remediation – the correction of something bad or defective; the action of remedying something, especially the reversal or stopping of damage to the technical and digital environment.
- Executive Summary – A Brief, comprehensive summarized business document with key points identified.

- IT Response – an answer or reply via basic communication channels, in words or in some action. Channels include but are not limited to digital, interpersonal, written, verbal, and physical communication.
- IT Incident – An attempted or successful unauthorized access, use, disclosure, exposure, modification, destruction, release, theft, or loss of sensitive, protected, or confidential information or interference with systems operations in an information system.
- Integrity – soundness of moral principle and character, as shown by one person dealing with others in the making and performance of contracts, and fidelity and honesty in the discharge of trusts.
- Professional Decorum – a dignified propriety of behavior, speech, dress, etc.; the quality or state of being decorous, or exhibiting such dignified propriety; orderliness; regularity.
- Root Cause Analysis – the evaluation and identification of a cause for failure, problem or undesirable condition.

POLICY STATEMENT

1. The TTUHSC El Paso CIO has implemented an event management policy to establish an event response team (ERT) with authority to remediate events/issues/ incidents when other troubleshooting efforts have been exhausted, or concentrated efforts are required to address an event that is meets a criticality level defined in the event matrix.
2. The roles outlined in this policy include the role of primary collaborator, event response team (ERT) team members, core personnel, and departmental team members.
3. In the event the executive member of the ERT team is unavailable, the lead role will default to the delegate defined in the TTUHSC El Paso IT Continuity of Operations Plan (COOP).
4. The ERT team policy is governed and enforced by the office of the TTUHSC El Paso CIO and is limited to personnel from TTUHSC El Paso Information Technology (IT) Department.
5. ERT Members as well as other IT personnel are expected to adhere to departmental policies, standards, and guidelines at all time during the event resolution policy.
6. All IT personnel are expected to be compliant with all aspects of the event management policy and align with security policies such as but not limited to: acceptable use of information resources, TAC 202, HIPAA, NIST, GLBA, and HITECH, during the remediation process.
7. The event management policy can be revised in the event of departmental changes to the event resolution process, required changes stemming from business continuity recommendations, or required changes from Human Resources Department to comply with Fair Labor Standards Act.

Event Management workflow Procedure

Event management is as follows:

1. The person to receive the initial request/event information will serve as the primary communicator/collaborator for the request. This designation is non-transferrable even if the event does not fall into troubleshooting for your specific area and job description. This designation requires that you will be responsible for communicating with the event management/response team and you will see the event request through to resolution. “Follow through” does not denote management and delegation authority or position of power over others but in fact refers to serving as primary collaborator. Primary collaborator involves engaging those groups necessary to assist in performing root cause analysis and resolving the event or issue.
2. The primary collaborator will convene the ERT when:
   a. All troubleshooting efforts have been exhausted; and
   b. The event has reached a criticality level of 5 or higher; or
   c. The event has demonstrated characteristics of an incident that can be escalated to a disaster.
3. The primary collaborator must engage *and* communicate all of the initial troubleshooting details to the ERT and follow up with all team members that need to be actively engaged. As an IT professional, all members of the ERT are expected to be able to report basic troubleshooting details such as the following:
   a. Date
   b. Time
   c. System name
   d. Application name (if necessary)
   e. Description of error

    f. IP address (if necessary)
    g. Requestor name
    h. Requestor eraider
    i. Description of troubleshooting details. These details include testing on different browsers, testing off the network, checking to see if the user has typed in the words on the link correctly, et cetera.
4. The primary collaborator will assess the event and determine severity level to convene the ERT.
5. The ERT will confirm severity level, develop an action plan for root cause analysis, and create a remediation plan.
6. ERT will report initial findings and action plan to the CIO, and begin remediation.
7. The primary collaborator will follow up with reports in 24, 48, and 72-hour increments depending on the severity and impact of the event.
    a. The primary collaborator for the event management/response team will follow the internal as well as external communication protocol as defined by the office of the CIO. Deviating from the established plan, compromising confidentiality and information integrity, and/or deliberate disregard of confidentiality from the CIO will result in disciplinary action.
8. The primary collaborator will develop a final report of root cause analysis, remediation, and resolution summary to IT leadership and CIO.
9. The primary collaborator will upload the resolution document into an IT knowledge base at the conclusion of the event resolution.
10. The document repository will be maintained by the helpdesk and populated by the primary collaborator.
11. If the event is classified as highly critical or time sensitive, the primary collaborator/response team must notify the CIO.
12. The CIO must be notified every instance that the event response team convenes.

EVENT MANAGEMENT GUIDELINES

1. Workflows and processes will be carried out using a root cause analysis framework to manage and remediate events.
2. Findings for events will be delivered in the form of an executive summary and stored in a document repository for IT to access as part of a knowledgebase for future reference. The document is required to be reviewed and approved by one representative from **each** core team section in order to be stored in the repository. Approval can be done via email but the email approval needs to be added into the last page of the document.
3. Events will be managed and addressed according to the following event matrix:

Severity Levels

Level	Description	Score
Critical/Urgent	Clients live system is at a halt and unable to process data, Critical business impact, network or environment is down, multiple users are directly affected, resources does not function as intended, end user is unable to perform some significant job function, a temporary workaround, alternative, or circumvention is not available, end user has an active service contract.	1
High	Serious disruption of a business function that limits the clients ability to conduct some portion of production business, Server or network response time impacting business applications, operation of an existing network or environment is severely degraded or significant aspects of end users operation are negatively impacted by unacceptable performance, the resource has limited functionality, the end user is unable to perform some small job function, a temporary workaround, alternative, or circumvention is available.	2

Level	Description	Score
Medium	Clients live system continues to run without serious impact on production business, operation of the network or environment is impaired although most business operations remain functional, a software, hardware, system or component installation/upgrade is necessary, a design/functional change is requested.	3
Low	Minor application issue, all questions and requests for information on use or implementation of software, Non-critical hardware/software enhancement, there is little or no impact to end user's business operation, non-time sensitive issues, general inquiries or maintenance and support required at a later date.	4

Population Impacted

Score	Population Types
4	Internal to IT
3	User
2	Departmental
1	Institutional

4. An event management/response team will include exempt members from a core group defined as Networking, Systems, Information Security, and PC Support and Classroom Technology. Additional members will include exempt members from application Development, Academics, DBA's, Research, and Clinical Information Systems.
   a. ERT members are assigned by the section supervisor and representatives from all areas are expected to be available to respond within 1 hour during work hours or 1-hour after hours to attend a WebEx session.
5. The use of the Event Response Team is to be used sparingly and only under conditions when all initial troubleshooting efforts have been exhausted. This expectation should also be considered when an event remediation collaborative session is scheduled outside of regular business hours.
6. Escalation: In the event that a member of the team that is necessary to resolve the issue does not respond by the 1-hour time frame, the issue will be escalated to the section director. In the event the team member does not respond within half an hour after it has been escalated, the issue will be escalated to the CIO.

While this policy is not an all-inclusive list of actions necessary to resolve an IT event, further clarification of expectations and workplace behaviors will be interpreted and communicated to IT personnel as scenarios require. All other IT Policies can be found at https://ttuhscep.edu/it/policies/

1. 56.50 Sanctions Policy.