# Site Personnel Cyberattack Response Procedures

The NCI Cancer Therapy Evaluation Program (CTEP) clinical trial systems house sensitive patient data, critical research information, and operational details vital to the success of clinical trials. Every staff member at a site participating in NCI trials plays an important role in the management and security of these systems. These procedures are designed to guide site staff in responding to cybersecurity incidents and protecting the systems and data; please follow these procedures if you experience a cybersecurity incident at your site.

1. **Report the cybersecurity incident**
    - Site staff should be familiar with their institution's security and security incident reporting policies. In the event of an incident, follow your institution's policy for reporting the incident and communicating the incident to outside entities including CTEP.
    - Reporting to CTEP: Following your institution's policy, report the incident to CTEP as soon as possible. The sooner we are informed, the faster we can respond to mitigate potential risks. **Report all incidents to:** CTEPsecurity@nih.gov and include the following information if available:
        i. Your contact information: name, phone and email;
        ii. Incident organization: Specify your organization or site;
        iii. The nature of the incident: Describe what you observed or experienced;
        iv. Systems involved: Identify the systems or workstations affected;
        v. Current status of the incident; and
        vi. Contact information for your IT department or relevant support.
        vii. Whether staff can access the email associated with their CTEP Identity and Access Management (IAM) account or if they are using an alternate email.

2. **Isolate your system**: Follow your organization's established guidelines to isolate your system/workstation from the network to prevent the spread of the incident to other systems.
3. **Deactivation of site user accounts**: In certain circumstances where a cyberattack could potentially impact CTEP systems, the CTEP Security team will deactivate site user accounts as a preventative measure to protect sensitive data and systems.
4. **Communication for specific requests**
   If you have any specific requests during the incident containment, please get in touch with us at: CTEPsecurity@nih.gov.
    - Patient care-related requests: If the requests are related to patient care, e.g., patient registration, drug orders, or SAE reports, we will address them manually.
    - Auditing-related requests: If the requests are related to auditing, the CTEP security team will report this to the NCI Information System Security Officer (ISSO) to assess the possibility of reactivating your account.
5. **Notification of Incident Resolution:** After the cybersecurity incident is resolved, please send us a notification from your IT department or any authorized departments to confirm the resolution.
6. **Reactivation of site user accounts**: Upon receiving notification of incident resolution from the IT or authorized departments, the CTEP Security team will promptly reactivate your user accounts.
7. **Provide Post-incident information**: After the incident is resolved, please provide us the post-incident information, including:

- Site functional impact: Describe how the incident affected site systems and users.
- Site data, files, or system damage.
- Anticipated documentation delays (e.g., serious adverse event reports, enrollments, or other critical documentation).
- Attack method.
- Actions/steps taken to contain the incident.
- Identified vulnerabilities in the system during or after the incident.