# Security Monitoring Policy:  Suspicious User Login Activity

## Overview

This policy establishes security monitoring processes and procedures for the event that suspicious login behavior is detected or reported. To mitigate potential cyber threats, we closely monitor and are alerted to suspicious login behavior via the various security tools we employ.

## Purpose

Security monitoring allows for the early detection of suspicious network login activity across the organization.  Early detection can block potential access to CIEE network resources before a breach or other security incident can occur.   The purpose of this policy is to ensure that security incidents such as suspicious login activity are reported, investigated, and mitigated to protect CIEE's assets.

## Scope

This policy applies to all staff with CIEE (full and part time staff, temporary staff, or any contractor staff) who have user accounts to access CIEE network and cloud-based resources and applications.

## Procedure

This procedure outlines the process followed when investigating any suspicious login activity detected or reported by or to the IT Security Team.

1. Suspicious activity (multiple invalid login attempts, login attempts flagged as unusual) is identified and IT Security Admins notified
2. A Security Admin will mark the alert as Under Investigation and begin researching the issue. (Jira)
3. If the Security Admin confirms that the log in is suspicious and is unable to determine the validity of the login, the user account in question will be locked.
    a. Once the user account is locked, the security Admin will notify the user's direct manager via email that the user account of a direct report has been disabled.
    b. The Manager will attempt to contact the user through an outside channel (personal email, phone, text, etc..) to determine if the user was trying to log in. The confirmation (yes or no) and any relevant details will be shared back with the Security Admin.
4. Security Admin will finish conducting a full investigation and will activate a disabled user account once all threats have been mitigated.
5. Security Admin will communicate to both the direct line manager and impacted user once complete.

Examples:

## Scenario 1:

1. Suspicious login behavior is detected by network monitoring tool.
2. Alert is sent to security admins including username of account displaying unusual behavior.
    a. Examples:
        i. exampleUser@ciee.org has attempted to login to Microsoft Outlook with an incorrect password multiple times.
        ii. exampleUser@ciee.org has attempted to login to Microsoft Outlook from an unusual location.
3. Security Admin(s) will review the alert and begin investigating the suspicious activity.
    a. Dependent on the severity of the suspicious behavior; IT may need to immediately disable/or block the user account in question.
    b. In the event that the user account is disabled/or blocked; the security admin will communicate this user account change to the user's direct line manager.
    c. The direct line manager will communicate to the individual user impacted and will provide any additional information received to the Security Admin who is leading the investigation.
4. Security Admin will conduct full investigation and will activate disabled/or blocked user account once all threats have been mitigated.
5. Security Admin will communicate to both the direct line manager and impacted user once complete.

## Scenario 2:

1. exampleUser@ciee.org receives a message from Microsoft asking them to confirm a new login attempt from an unknown device.
2. exampleUser@ciee.org who is working from their home office on their existing laptop and smartphone reports the incident to IT Support by submitting a ticket in Jira.
    a. exampleUser will provide secondary contact information (personal email, cell number, etc) in the Jira ticket.
    b. If exampleUser is unable to submit a ticket on their behalf due to disabled/or blocked user account, then direct line manager will submit ticket on their behalf. Direct Line Manager will include secondary contact information for the user impacted.
3. The ticket is assigned to the Security Admin who begins the investigation.
    a. Dependent on the severity of the suspicious behavior, IT may need to immediately disable/or block the user account in question.
4. Security Admin will conduct full investigation and will activate disabled/or blocked user account once all threats have been mitigated.
5. Security Admin will communicate to both the direct line manager and impacted user once complete.