Capital Chase Incident Response Policy

DOCUMENT PURPOSE
This document defines the policy for addressing Security Incidents through appropriate Incident Response. This document applies to all Personnel and supersedes all other policies relating to the matters set forth herein.

SCOPE
The objective of this policy is to ensure a consistent and effective approach to the management of Security Incidents, including communication of Security Events and Security Weaknesses.

INCIDENT RESPONSE POLICY
The Incident Response policy is as follows:

- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to Security Incidents.
- The objectives for Security Incident management should be agreed upon with management, and it should be ensured that those responsible for Security Incident management understand the organization's priorities for handling Security Incidents.
- Security Events should be reported through appropriate management channels as quickly as possible.
- Personnel and contractors using the organization's information systems and services are required to note and report any observed or suspected Security Weakness in systems or services.
- Security Events should be assessed and it should be decided if they are to be classified as Security Incidents.
- Security Incidents should be responded to in accordance with documented Incident Response procedures.
- Knowledge gained from analyzing and resolving Security Incidents should be used to reduce the likelihood or impact of future incidents.
- Procedures should be defined and applied for the identification, collection, acquisition, and preservation of information, which can serve as evidence.
- Awareness should be provided on topics such as:
    - The benefits of a formal, consistent approach to Incident Management (personal and organizational);
    - How the program works, expectations;
    - How to report Security Incidents, who to contact;
    - Constraints imposed by non-disclosure agreements.
- Communication channels should be established well in advance of a Security Incident. Include all necessary parties in relevant communication:
    - SIRT members
    - Senior Management
        - Capital Chase Personnel
- Individuals needed and responsible for responding to a Security Incident will include the following:
    - Transpeed IT Support
    - Hayley Lewis
- Other groups and/or individuals that may be needed include:
    - Senior management
    - Human Resources
    - End User Support
    - IT Production Staff
    - Building and/or facilities management staff
    - Other Personnel involved in the Security Incident or needed for resolution
    - Contractors (as necessary)