**1510: Notification/Escalation**

**Model Content Revised Date: 5/15/2024**

Incidents can begin in many forms. A beginning can be so small and innocuous that it escapes notice at first, it can be so large and calamitous that it instantly overwhelms any on-scene personnel, or it could fall anywhere between these extremes. While large calamitous incidents are easily recognized as likely disaster events, many times the worst disasters are those where a seemingly small and innocuous incident is left unchecked and spirals into something much bigger. Because of this, an effective and efficient Notification/Escalation process is the most vital component of the Incident Management plan.

The majority of incidents typically fall into one of two categories: Life Safety and Break/Fix. Each of these incident types has unique steps that should be followed. There is, however, a third incident type that is becoming increasingly prevalent in today’s technology-dependent world: a Cyber incident. Therefore, the first task of any personnel on the scene when an incident is discovered is to determine if the incident is a Life Safety, Break/Fix, or Cyber issue.

**If a Life Safety Issue –**

In a Life/Safety incident, the immediate concern is ensuring the safety of anyone on the scene. As such, the initial responses work towards that objective.

1. Ensure the safety of employees and visitors.
2. If appropriate, immediately evacuate the facility via the nearest available exit following the Evacuation Plan, or (if the danger is outside the facility), seek shelter in place inside the facility. Ideal locations are inside a secure, interior room of the facility, away from any standard windows and doors. The Vault offers even greater protection, with a concrete, windowless shell and steel fire doors.
3. Dial 911 to alert emergency response personnel of the situation. Give them your name and phone number, the address, the nature of the incident, and any injuries to anyone at the scene.
4. From your Emergency Wallet Card, contact ANY member of the Management Team to alert them of the situation. Provide them with the same details given to the 911 operator.
5. Management will alert the Incident Management team and/or establish an emergency Conference Bridge.

**If a Break/Fix Issue –**

In a Break/Fix incident, the immediate concern is to alert the appropriate individuals to respond to and either correct the issue before it becomes a critical event or to mobilize the appropriate resources and plans to minimize its impact and ensure the continuity of our business operations. As such, the initial responses work towards that objective.

1. Alert the appropriate vendor of the nature and scope of the incident:  
     
   {Insert contact information here, including local emergency contacts, vendors, etc. Include the name of organization, contact (if known), phone number, email, website, phone tree option numbers, etc - a sample list is below, but may not be all-inclusive}  
   1. Emergency Response (Police, Fire, and Ambulance)
   2. TruStage Insurance
   3. League/Association
   4. NCUA
   5. Federal Bureau of Investigation
   6. State Bureau of Financial Institutions
   7. Federal Reserve:
      * ACH Support
      * CU ABA Number:
      * After Hours Help Desk
   8. Key Vendor (add more as needed)
2. (Initial responder) Determine the impact and expected duration of the issue.
3. Escalate to the Management Team as appropriate.
4. Management Team to notify the staff as appropriate.
5. Establish an emergency Conference Bridge.

**If a Cyber Incident –**

1. Assess the nature and scope of the incident.
2. Notify the Management Team.
3. Management Team will assess the situation and execute initial cyber incident response procedures.
4. Management Team will alert the Cyber Incident Response Team.
5. The Cyber Incident Response Team will assess the situation and take steps to contain and control the incident.
6. Preserve records and other evidence.
7. Notify regulatory/law enforcement authorities (new rules require initial NCUA notification within 72 hours).
8. File Suspicious Activity Reports (SARs) for fraudulent activity related to the incident.
9. (When warranted), notify impacted members.

*NOTE: Reference the Cyber Incident Response information (Section 1600) for further details, resources, and information.*