Process for the mitigation of Cyber security incident

A Cyber Security incident is defined as meeting one or more of the following conditions:

- Any potential violation of Federal law, New Mexico law, City ordinance or City rule, regulation, Administrative Instruction or policy involving a City information technology asset.
- A breach, attempted breach or other unauthorized access of a City information technology asset. This could be a computer virus or malware which purpose is to disrupt or steal information.
- Any conduct using in whole or in part a City information technology asset which could be construed as harassing, or in violation of City policies.
- Evidence of tampering with City data or computer hardware.
- Other incidents that could undermine or raise concern about the availability, stability, reliability or integrity of the City's information technology infrastructure.

1. A Security Incident is discovered by alert from external source or reported by internal staff

2. Notify IT Security or the ITSD Service Desk of incident immediately

3. ITSD Security working with ITSD Service desk - Triage incident to determine level of risk to infrastructure, Levels of alert:

   Red, has high potential of affecting critical resources and majority of staff within the City of Albuquerque
   Yellow, has potential to affect specific resources or staff
   Green, for notification purposes only

4. IT Security/ITSD Service Desk - Evaluate incident to determine appropriate staff to lead mitigation effort.

5. ITSD Security or Service Desk creates incident ticket documenting potential vulnerability, who it affects and mitigation efforts if applicable.

6. Assign Incident manager; submit ticket to assigned incident manager.
   For Red incident, notify incident response members and CIO/DCIO

7. Incident manager – Develop procedures for mitigating risk, if procedures require additional staff or other resources, document staff and resources required.

8. Incident manager – Take appropriate action necessary to mitigate risk

9. Incident manager – Document actions taken. For a red alert, notify incident response members of mitigation efforts.

10. Incident manager – For Red incident, develop and prepare to present an After Action Report.

11. Close Ticket.