**1. Preparation:**

* Ensure that all necessary security controls are in place, such as multi-factor authentication, strong passwords, and access controls.
* Ensure that an incident response plan is in place and regularly reviewed and tested.
* Establish a dedicated incident response team and identify their roles and responsibilities.
* Ensure that all employees are trained on cybersecurity best practices and know how to report incidents.

**2. Detection:**

* Monitor logs and network traffic for signs of compromise, such as unauthorized access attempts or unusual account activity.
* Use intrusion detection and prevention systems to detect and block malicious traffic.
* Conduct regular vulnerability assessments and penetration testing to identify and remediate vulnerabilities before they can be exploited.
* Train employees to recognize and report suspicious activity, such as phishing emails or social engineering attempts.

**3. Containment:**

* Isolate the affected account and disable it.
* Change the password for the affected account and any other accounts that share the same password.
* Identify and isolate any affected systems or networks.
* Deploy software or hardware firewalls to block any malicious traffic.

**4. Investigation:**

* Conduct a thorough investigation to determine the scope of the compromise and the root cause.
* Collect and preserve evidence, such as logs and network traffic.
* Analyze the evidence to determine the attacker's methods, the extent of the compromise, and any data loss or exfiltration.

**5. Eradication:**

* Remove any malicious software or code that may have been installed.
* Patch any vulnerabilities or misconfigurations that were exploited.
* Ensure that all systems and networks are secure before restoring them to normal operation.

**6. Recovery:**

* Restore any affected systems or networks to normal operation.
* Monitor logs and network traffic to ensure that the attacker has been fully eradicated.
* Verify that all systems and networks are fully patched and up to date.

**7. Lessons Learned:**

* Conduct a post-incident review to identify any areas for improvement in the incident response plan.
* Update the incident response plan based on lessons learned.
* Conduct additional training for employees on cybersecurity best practices and incident response.

It is important to note that this is a general framework and that specific incident response plans should be tailored to the individual organization's needs and circumstances.