1. The first step will be detection; you'll use security information and event management (SIEM) tools to scan for unusual activity on the network. Some SIEM tools are Security Onion, the ELK stack, and Graylog. Inform employees to report unusual or suspicious activity on their devices immediately.

2. The next step will be analysis, assess the reported issue to understand the nature and scope of the potential attack. Collect evidence, such as logs, screenshots, and other relevant data from the affected device. Identify what sensitive data may have been accessed or compromised.

3. The third step will be containment, disconnect the compromised device from the network to prevent the spread, and apply temporary firewall rules or access controls to limit exposure.

4. Step four: eradication, remove malicious software using antivirus and anti-malware tools, identify and patch any vulnerabilities that were exposed during the attack, reset passwords for affected logins, and implement stronger authentication measures.

5. Roles and responsibilities. Coordinate the response efforts, security analysts analyze the breach, collect evidence, and assist in eradication efforts; IT support offers technical support to isolate compromised systems and enforce security measures; compliance officer oversees adherence to data protection regulations and prepares required reports for regulatory bodies.

6. Post-incident review, debrief staff after the incident has been resolved, what could have been done better, and update and revise the incident response policies.