SCHOOL SECURITY BREACH

1. Preparation:

Develop a comprehensive Incident Response Plan (IRP):

Firewall detection system to warn system breach and any authorized data access and app. Blocking the social media for the entire school internet system.

Conduct regular security audits and vulnerability assessments:

These assessments help identify weaknesses in the system and allow for proactive measures to be taken.

Provide security awareness training to employees:

Educating employees about security threats and proper procedures can help prevent breaches and enable them to recognize suspicious activity.

Implement robust security controls:

These controls may include firewalls, intrusion detection systems, anti- malware software, and access controls.

2. Detection:

- **Monitor for suspicious activity:** Utilize security tools and processes to monitor for unusual patterns or behaviors that could indicate a breach.
- **Establish clear reporting procedures:** Employees should know how to report suspected security incidents and what information to provide.
- **Review security logs and alerts:** Regularly analyze security logs and alerts to identify potential threats.

3. Analysis and Identification:

- **Investigate the breach:** Determine the scope, impact, and cause of the incident.
- **Gather evidence:** Collect relevant data, such as security logs, system images, and network traffic, to help in the investigation.
- **Analyze the data:** Use tools and techniques to analyze the data and identify the root cause of the breach.

4. Containment:

- **Isolate affected systems:** Immediately isolate systems that have been compromised to prevent further damage.
- **Limit access to affected areas:** Restrict access to systems and data that are under investigation.
- **Disable compromised accounts:** Disable accounts that may have been compromised by the attacker.

5. Eradication:

Remove malicious software or code:

Eliminate the cause of the breach by removing malware or other malicious code. Implement patches and updates:

Apply necessary security patches and updates to address identified vulnerabilities.

Restore compromised systems:

Restore affected systems to a secure state using backups or other recovery methods.

6. Recovery:

- **Restore data:** Recover lost or damaged data using backups or other recovery methods.
- **Re-establish systems:** Return systems to their operational state after the breach has been addressed.
- **Implement preventative measures:** Strengthen security controls and implement new security measures to prevent future breaches.

7. Post-Incident Review:

Conduct a post-incident review:

Analyze the lessons learned from the incident and make recommendations for improvements.

Update the Incident Response Pl

Revise the plan based on the post-incident review and incorporate new security measures.

MANUAL CAMPUS SHUTDOWN

1. Planning and Communication:

Identify critical systems, essential personnel, and necessary resources for the shutdown.

- **Communicate the plan effectively:** Inform staff and students about the shutdown schedule, procedures, and emergency contact information.

Shutdown checklist: Outline specific tasks for each department and building.

2. Securing Buildings:

- **Close and secure buildings:** Ensure all doors and windows are locked, and security measures are in place.
- **Set out-of-office notices:** Update email and voicemail messages to reflect the shutdown period.
- **Turn off non-essential equipment:** Unplug fans, heaters, and other devices not needed for essential operations.

3. Preparing Essential Systems:

- **Verify proper operation of building systems:** Ensure fire alarm systems, elevators, and other essential systems are functioning correctly.
- **Prepare for reduced staffing:** Identify essential personnel and their roles during the shutdown period.
- **Plan for potential emergencies:** Have a clear plan for responding to emergencies during the shutdown.

4. Laboratory Shutdown:

. **Secure laboratory equipment:** Close fume hoods, secure chemical bottles, and turn off non-essential electrical devices.

. **Prepare for emergency situations:** Identify potential hazards and have a plan for responding to them.

. **Secure animals and equipment:** If applicable, take special precautions to secure experimental animals and equipment.