GAT labs

TEMPLATE

CYBERSECURITY

Incident Response Plan (CSIRP)

CYBERSECURITY

Incident Response Plan

Instructions for Using the Incident Response Plan Template

1. Fill in Organisation Details: Provide accurate information about your organisation, including the main contact person for the CSIRP. This information will be crucial for quick communication during an incident.

2. Incident Identification: Tick the applicable box to classify the type of incident encountered. Add any specific details in the 'Other' section if the incident type isn't listed.

3. Initial Response: Follow the steps to ensure that the incident is managed promptly. Document all actions taken for later review.

4. Incident Containment: These actions prevent the spread of the incident. Isolating affected systems is critical to protect unaffected areas of the network.

5. Incident Eradication: Identify and eliminate the root cause of the incident to prevent recurrence. This may involve removing malware or repairing security flaws.

6. Recovery: Restore operations by recovering data from backups and testing the systems to ensure they function correctly. Monitor the systems for any signs of weakness that could be exploited again.

7. Communication: Maintain clear and open communication with all stakeholders. This includes internal teams and, if necessary, external stakeholders such as customers or the public.

8. Post-Incident Review: After the incident is resolved, conduct a thorough review to identify lessons learned and areas for improvement. Update the CSIRP as needed.

9. Approval and Implementation: Ensure that the plan is approved by the appropriate authority within your organisation. Set review dates to keep the plan updated.

10. Regular Testing: Regularly test the plan using simulated incidents to ensure everyone knows their role and the procedures work as intended.

Company Name

IRP Contact Person

Address

Contact Info.

1. Incident Identification:

- □ Suspected data breach
- □ Ransomware attack
- □ Loss or theft of equipment
- □ Unauthorised access

Other: ____________________

2. Initial Response:

- □ Notify incident response team
- □ Document the incident details
- □ Assess the initial impact

3. Incident Containment:

- □ Isolate affected systems
- □ Secure backup data
- □ Change passwords and access codes

4. Incident Eradication:

- □ Identify the cause of the incident
- □ Remove malware
- □ Repair system vulnerabilities

5. Recovery:

- □ Restore systems from clean backups
- □ Test system functionality
- □ Monitor for further disruptions

6. Communication:

- □ Notify affected parties
- □ Communicate with stakeholders
- □ Prepare public statement (if necessary)

7. Post-Incident Review:

- □ Conduct a post-mortem analysis
- □ Update the IRP based on findings
- □ Provide training updates

Notes:

Approved by:

Date: