Handling Inappropriate Usage Incidents

Objectives:

At the end of this episode, I will be able to:

Understand what inappropriate usage incidents are.

Explain what the different techniques that IH&R team members may use during an investigation detect inappropriate usage incidents are.

Identify what steps the IH&R team should take to contain and eradicate inappropriate usage incidents.

Define what the steps that the IH&R team should take to ensure recovery from inappropriate usage incidents.

External Resources:

Handling Inappropriate Usage Incidents

What is an Inappropriate Usage Incident? -

Incidents in which a user violates the acceptable computing use policies.

What techniques can the IH&R team use to detect Inappropriate Usage Incidents? -

```
▪ Detecting High Resource Utilization
▪ Accessing Malware in the Network
▪ Reviewing Log Entries of Application Logins
▪ Analyzing Network Security Device Logs
```

What steps should be taken to Contain Inappropriate Usage Incidents? -

Recommendations for containing Inappropriate Usage Incidents include:

```
▪ Turn off all the malware infected systems present in the network immediately
▪ Filter the ports and secure the protocols that are affecting the network
▪ Install URL / spam filtering software on the email server
▪ Block malicious website URLs
▪ Limit privileges of employees to prevent installation and spreading of
malicious or unwanted programs
▪ Change passwords for the accounts misused and track the activity of the
users involved
```

What steps should be taken to Eradicate Inappropriate Usage Incidents? -

Recommendations for eradicating Inappropriate Usage Incidents include:

```
▪ Install firewalls and IDPSs to block services that violate the
organization’s policies

▪ Configure the email servers to attempt to block outbound spam

▪ Use a web proxy server that runs URL filtering software to prevent access to
inappropriate or malicious websites

▪ Configure firewalls to send ALL outgoing requests through proxy servers
```

What steps should be taken to Recover after Inappropriate Usage Incidents? -

Recommendations for Recovering after an Inappropriate Usage Incidents include:

```
▪ Consult with human resources and the legal department regarding the procedures
to handle inappropriate usage incidents

▪ Provide training to ALL employees to ensure awareness of policies

▪ Provide proper guidelines and policies about downloading content using the
organization's systems and networks

▪ Keep antivirus software signatures updated
```