Incident Identification and Reporting Details

Incident Information

Incident ID:
INC-2024-017

Date & Time of Incident:
2024-06-10, 14:45

Location:
Server Room B2, Main Office

Reported By:
Alex Morgan

Department:
IT Operations

Incident Description

Summary:
Unauthorized access detected on database server.

Details:
At approximately 14:30, monitoring systems flagged multiple failed login attempts followed by a successful connection from an unknown IP address. The affected server is hosting confidential data for internal applications. Immediate steps were taken to restrict access and preserve system logs for further analysis.

Immediate Actions Taken

Containment:
User accounts on the affected server were disabled, and the server was disconnected from the network.

Notification:
Incident reported to Security Team Lead and System Administrator.

Preservation:
Server logs and related evidence preserved for investigation.

Further Reporting

Status:
Under Investigation

Date/Time Reported:
2024-06-10, 15:05

Reported To:
Jane Lee (CISO)

Important Notes

- All incidents must be reported as soon as detected, following organizational procedures.
- Details should be factual and clear; avoid speculation.
- Preservation of digital evidence is vital for investigation.
- Only authorized personnel should access and handle incident information.
- Timely response and documentation are critical for minimizing impact.