Recommended

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

INCIDENT RESPONSE POLICY AND PLAN

POLICY: F48

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview

In accordance with security best practices, all security incidents will be formally documented and responded to. This policy provides some general guidelines and procedures for dealing with computer security incidents.

Purpose

The WCUUSD is committed to maintaining the security of electronic information. Formal practices of tracking and mitigating security incidents will aid in assessing potential risks and vulnerabilities to data. As such, WCUUSD will continually assess risks and improve security measures.

Incident Examples

Some examples of possible incident categories include:

- Compromise of system or data integrity
- Denial of system resources.
- Illegal access to a system (either a penetration or an intrusion).
- Malicious use of system resources
- Inadvertent damage to a system.
- Malware or virus detection.

Some possible scenarios for security incidents are:

- Loss of a laptop or device containing, HIPAA, PII and/or other WCUUSD – data.
- Suspicious activities or anomalies that are identified through intrusion detection, firewall or other network device logs. You have discovered a major virus has infected multiple systems.
- Damage, intentional or accidental, to equipment or system affecting its ability to perform its job.
- Unauthorized wireless access points.

Incident Reporting

All suspected policy violations, system intrusions, virus infestations, and other conditions which might jeopardize WCUUSD information or WCUUSD information systems must be immediately reported to the WCUUSD Information Technology Helpdesk (ithelp@u32.org), who will coordinate with the WCUUSD Director of Technology and/or Superintendent.