IT Vulnerability Assessment Policy

POLICY NUMBER: ADM-3012

RELEASE DATE: April 9, 2021

SUPERSEDES: N/A

PURPOSE

The purpose of this policy is to grant authorized entities access to WorkForce Central's networking, computing, and information resources for the purpose of conducting audits, including vulnerability assessments and penetration tests.

BACKGROUND

Security audits assess WorkForce Central's security stance against an organized listing of security protocols, strategies, and procedures to ensure its IT infrastructure is secure and protected against data breaches.

Audits may be conducted to:

- Investigate possible security threats.
- Test the security of information systems.
- Make sure that the information is only accessible by the individual who should be able to access it.
- Make sure system is protected from any unauthorized modification.

A standard security audit will evaluate the following:

- Email
- Information handling processes
- Hardware configurations
- Data and access-related details (i.e., cards, tokens, passwords)
- User practices
- The physical configuration of the system and setting
- Network
- Software configurations
- Smart devices

POLICY

WorkForce Central will review this policy on an annual basis to ensure proper security procedures are being followed.

If the results of the security audit result in an identified weakness, WorkForce Central will act immediately to resolve the issue.

Endpoint Protection

- A laptop device that is assigned and managed by WorkForce Central must use IT management approved endpoint protection software and configuration.
- The endpoint software must not be altered, bypassed, or disabled.
- Controls to prevent or detect the use of known or suspected malicious websites must be implemented.

Patch Management

- WorkForce Central's IT Team is responsible for patch management, operations, and procedures.
- All devices must be scanned on a regular basis to identify missing updates.
- All missing software patches must be investigated by the WorkForce Central IT Team.
- The status of the software deployment must be periodically checked.

Penetration Testing

- Penetration testing of the internal network must be conducted annually.
- Exploitable vulnerabilities found during the assessment will be corrected and re-tested by WorkForce Central's IT Team.

Approved Scanning Tools

Scanning tools used to perform vulnerability assessments must have documented justification and requires written approval by the WorkForce Central IT Team.

Periodic Vulnerability Assessment

WorkForce Central will conduct vulnerability assessments on an annual basis. The tools used to scan and assess must be enterprise-class. The tools used must be capable of scanning the systems from a central location and be able to provide remediation suggestions.

- Scans must be performed during appropriate business hours and minimize disruptions to normal business functions.
- All data from scans are to be treated as confidential.
- WorkForce Central will not make any temporary changes to the internal systems for the purpose of passing the vulnerability assessment. Any attempt to tamper with the results will be referred for disciplinary action.
- Devices that are connected to the WorkForce Central network must be specifically configured to block vulnerability scans from authorized scanning engines.

Remediation and Compliance

WorkForce Central shall receive a Mitigation and Compliance Report at the conclusion of the annual vulnerability assessment. The report will summarize the following:

- List of vulnerabilities: Detected vulnerabilities affected information systems, and the severity of the vulnerability.
- Remediation steps: Every weakness found during the assessment will have listed detailed information on how to eliminate the vulnerability.
- Timeline for completion of the remediation steps.

WorkForce Central's IT Team will remedy and/or mitigate discovered vulnerabilities based on the following rules:

- "High" or "Critical" level vulnerabilities will be addressed within two (2) calendar days of discovery.
- "Medium" level vulnerabilities will be addressed within ten (10) calendar days of discovery.
- "Low" level vulnerability will be addressed within 30 calendar days of discovery.

DEFINTIONS

Information System-Software, hardware, and interface components that work together to perform a set of business functions.

Penetration Testing (ethical hacking)- Practice of testing a network, computer system, or web application to find security vulnerabilities that an attacker could exploit.

APPROVED

Katie Condit

Katie Condit (Apr 9, 2021 09:16 PDT) Apr 9, 2021

Kate Condit, WFC CEO Date