Administrative Policies

IT Vulnerability Assessment Policy

POLICY #:	*ADM-3012, Rev. 1*
EFFECTIVE:	*July 29, 2025*
SUPERSEDES:	*IT Vulnerability Assessment Policy ADM-3012, effective April 9, 2021*

PURPOSE:

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

The purpose of this policy revision is to:

- Remove annual policy review requirement.
- Non-substantial edits for clarity.

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.
- Ensure information is only accessible to the individual authorized to access it.
- Ensure the system is protected from unauthorized modification.

A standard security audit will evaluate the following:

- Email
- Information handling processes
- Hardware and software configurations
- Data and access-related details (i.e., cards, tokens, passwords)
- User practices

- Physical configuration of the system and setting
- Network
- Smart devices

POLICY:

WorkForce Central will 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 to and managed by WorkForce Central must use IT management approved endpoint protection software and configuration. The 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 Department 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 Department. 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 retested by the WorkForce Central IT Department.

Approved Scanning Tools

Any external organization performing vulnerability assessments for WorkForce Central must provide documented justification and obtain written approval from the WorkForce Central IT Department for the scanning tools used.

Periodic Vulnerability Assessment

WorkForce Central will conduct vulnerability assessments on an annual basis. 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.

The tools used to scan and assess must be enterprise-class, be capable of scanning the systems from a central location, and be able to provide remediation suggestions.

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 known to be sensitive to scanning should be reviewed and may be excluded from vulnerability scans to avoid potential disruption.

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 detected vulnerabilities affected information systems and the severity of the vulnerabilities.
- Remediation steps. Every weakness identified during the assessment will have listed detailed information for how to eliminate the vulnerabilities.
- Timeline for completion of the remediation steps.

WorkForce Central's IT Department 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 vulnerabilities will be addressed within 30 calendar days of discovery.

Definitions

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.