Clark County Can Improve VPN Security

Audit Department

July 2025

togetherforbetter

Background

- A Virtual Private Network (VPN) is used by Clark County employees, consultants, and vendors, to securely access the Clark County network.
- Over the past several years, the number of individuals using VPN to access the County network increased substantially due to an increase in remote work options. There are currently 3,603 employees and 170 vendors connected to the County network.
- State law requires Clark County to follow specific cybersecurity controls. Clark County follows guidelines issued by the Center for Internet Security to comply with this law.
- Clark County is also subject to other requirements for securing data. These include the HIPAA Privacy and Security Rule, Payment Card Industry standards, and Criminal Justice Information System standards.

Objectives

- Determine whether VPN implementation and configuration are appropriate.
- Verify that policies and procedures are adequate to protect County data.
- Ensure Clark County maintains user permissions based on employment status and job duties; and
- Determine whether VPN activity is monitored.

Conclusion

We found that while VPN applications used by Clark County are generally configured appropriately, there are areas that can be improved.

These include:

- Completion of risk assessments;
- Application of pre-connection security requirements;
- Disabling of dormant accounts;
- Selection of alert criteria;
- Completion of policies and procedures; and
- Testing of backup procedures.

#1- Risk Assessment Was Not Completed for VPN (High)

Risk assessments identify scenarios that could affect the availability, confidentiality, or integrity of data. HIPAA regulations also require risk assessments. Organizations can be fined for not conducting risk assessments. Without a completed risk assessment, we could not determine whether Clark County properly identified and mitigated risk areas.

Recommendations

- Complete a written risk assessment for VPN applications to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data.
- Implement additional security measures as appropriate based on the assessment.
- Review and update the risk assessment annually to ensure risks are at reasonable and appropriate level.

#1 - Risk Assessment Was Not Completed for VPN

Management Response and Corrective Action Date

- The Enterprise Information Security team will create and complete a risk assessment for the two VPN applications no later than August 14, 2025.

#2 – Security Requirements to Connect to the County Network by VPN Do Not Apply to All Users (High)

Clark County has certain requirements users must meet to connect to the County network through VPN. Requirements include items such as antivirus, antispyware and firewall software that must be installed on the host. We found that the County is not requiring all user types to comply with these requirements.

This creates a risk that a user does not comply with the requirements, subjecting the County to greater risk of virus, spyware, or unapproved access.

Recommendation

Verify all clients connecting to County VPN have the latest version of Windows with critical security updates installed and an antivirus package with an up-to-date virus signature database.

#2 - Security Requirements to Connect to the County Network by VPN Do Not Apply to All Users

Management Response and Corrective Action Date

- Information Technology team will work to implement endpoint posture assessment for Operating System patches and antivirus checks on the VPN. The initiative will require planning, testing, training, and documentation to support a smooth deployment. We anticipate completing this work by November 1, 2025.

#3 – Dormant Accounts Not Disabled within CIS Required Timelines (Medium)

Clark County disables accounts after 60 days of inactivity. CIS controls require accounts be disabled after 45 days of inactivity. The longer time period increases the risk that an account is compromised.

Recommendation

Update the current process to disable accounts after 45 days of inactivity

Management Response and Corrective Action Date

Information Technology team will update our current process to disable accounts after 45 days of inactivity as suggested. This will be completed by September 1st, 2025.

#4 – Criteria for Automated Log Reviews Needs to be Validated (Medium)

Clark County IT uses an application to automatically review logs based on criteria set by the department. They also perform manual reviews of logs as needed. We could not determine if Clark County IT included all appropriate scenarios in the automated review. IT should have identified these types of scenarios during a risk assessment.

Recommendation

Review and update automated log reviews based on risks identified in risk assessment.

#4 – Criteria for Automated Log Reviews Needs to be Validated (Medium)

Management Response and Corrective Action Date

- Clark County Information Technology (CCIT) department has a number of tools in place that can detect anomalous login activity. The primary tool is a SIEM platform. The tool ingests a number of logs from various sources and correlates events from each log to identify anomalous behavior. This includes multiple logins from disparate geographical locations and\or times.

- CCIT was already migrating to a new SIEM which offers a more robust and granular platform. During this migration, additional logs, rules and alerts will be added. There are additional tools that could also detect anomalous logins. Finally, CCIT has monitoring \ alerting engagements with both MS-ISAC and our contracted security services partner to identify and alert CCIT when anomalous behavior is detected on the network.

- Completion of the migration to the new tools will ensure the appropriate logs and alerts are configured to maintain the appropriate probability that anomalous behavior is detected and the appropriate alerts are generated.

#5 – Policies and Procedures Need to Be Updated (Low)

We found several policies and procedures related to VPN did not accurately reflect current practices or were incomplete.

Recommendations

Update existing policies and procedures to ensure they reflect current practices.

#5 – Policies and Procedures Need to Be Updated (Low)

Management Response and Corrective Action Date

Clark County Information Technology (CCIT) has an active project to evaluate and migrate our EDR (Endpoint Detection & Response) from our current solution to another solution. We are targeting the end of September 2025 to complete this effort.

The new tool has additional features that CCIT will evaluate and implement, as appropriate, in an effort to further enhance this tool and as a regular part of the ongoing tuning and management of the platform. All appropriate and necessary policies and procedures will be developed to support the new tool.

CCIT also has an existing effort underway to significantly enhance the e-mail security platform. Updates will be made to the phishing incident response runbook. We expect to complete these efforts by September 30th, 2025.

#6 – VPN Related Issues are Not Resolved In Accordance with Department Guidelines (Low)

Clark County IT prioritizes issues reported to the help desk and has timelines established for resolution of each type. A "ticket" is opened for each issue and assigned to the responsible technician. There were 407 incidents related to VPN services during fiscal year 2024. We sampled a total of 41 incidents and found 11 out of 41 (27%) tickets related to VPN services did not meet the target response times (1 priority 1, 3 priority 2, and 7 priority 3). VPN incidents should be resolved in a timely manner to reduce potential security issues, including unsecure user work arounds and lost work time while waiting for an issue to be fixed.

Recommendations

- Create a written policy or procedure that provides directions to Clark County IT employees for actions to take when tickets are assigned to them. Include Inactivity alerts to ensure that the tickets are addressed according to target response times.
- Review the target response times to ensure they meet current business needs.
- Create an additional priority for items that are low priority and require longer than the current priority 3 response time to minimize inactivity alerts fatigue.

#6 – VPN Related Issues are Not Resolved In Accordance with Department Guidelines

Management Response and Corrective Action Date

CCIT is reviewing and will update processes related to incident and problem management. An additional priority level for lowest-level priority incidents will be created. Training and ongoing monitoring of incident response will be provided to all employees that are assigned incident tickets.

#7 – Backup Data for VPN Applications Should be Tested Periodically (Low)

During our testing, we found that while Clark County IT has a detailed recovery process for recovering and restoring a server, they do not have a process in place to test the backup. CIS Control 11.5 requires organizations to test backup and recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Recommendations

Implement a procedure to ensure backups are tested or used for recovery at least quarterly or conduct a risk analysis to determine that it is not needed.

Management Response and Corrective Action Date

CCIT will conduct a risk analysis and review and update the backup and recovery protocols for the VPN service and services / appliances and include testing of the backups on a basis that conforms to CIS Control 11.5.