

# Security Assessment

## Risk Report



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: TEL5

Prepared by: TEL5

07/08/2025

Scan Date: 07/08/2025

# Table of Contents

01	Discovery Tasks
02	Risk Score
03	Issues Summary
04	Unrestricted Web Content
05	Local Security Policy Consistency
06	Dark Web Scan Summary

# Discovery Tasks

The following discovery tasks were performed:

TASK	DESCRIPTION
✓ Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
✓ Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
✓ Detect User Controls	Determines if controls are in place for user web browsing.
✓ Detect Wireless Access	Detects and determines if wireless networks are available and secured.
✗ External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and categorizes external security threats.
✓ Network Share Permissions	Documents access to file system shares.
✓ Domain Security Policy	Documents domain computer and domain controller security policies.
✓ Local Security Policy	Documents and assesses consistency of local security policies.

# Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

# Issues Summary

This section contains summary of issues detected during the Security Assessment. It is based on general industry-wide best practices and may indicate existing issues or points of interest. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.

## Overall Issue Score

Current  907

**Overall Issue Score:** Risk Score x Number of Incidents = Total points: Total percent (%)

### 250 Compromised Passwords found on the Dark Web (50 pts each)

**Current Score:** 50 pts x 5 = 250: 27.56%

**Issue:** A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2021.

**Recommendation:** Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess. Only the first 5 per domain are listed here.

### 225 Passwords less than 8 characters allowed (75 pts each)

**Current Score:** 75 pts x 3 = 225: 24.81%

**Issue:** Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.

**Recommendation:** Enable enforcement of password length to 8 or more characters.

### 216 Password history not remembered for at least six passwords (72 pts each)

**Current Score:** 72 pts x 3 = 216: 23.81%

**Issue:** Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.

**Recommendation:** Increase password history to remember at least six passwords.

## 216 Automatic screen lock not turned on (72 pts each)

**Current Score:** 72 pts x 3 = 216: 23.81%

**Issue:** Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.

**Recommendation:** Enable automatic screen lock on the specified computers.

# Unrestricted Web Content

The assessment examined whether computers employ web content filters. The percentages below represent the number of potentially unsafe websites that are unrestricted by content category. A higher score indicates that users have unrestricted access to multiple websites that may pose a security threat. \*Note that this data does not reflect the actual browsing activity of employees or users on the network.

## Content Filtering Assessment



# Local Security Policy Consistency

## % Policy Consistency





# Dark Web Scan Summary

The following results were retrieved using a preliminary scan of the Dark Web using ID Agent ([www.idagent.com](http://www.idagent.com)).

Only the first 5 per domain are listed here.

EMAIL	PASSWORD/SHA1	COMPROMISE DATE	SOURCE
varun@tel5.com.au	Ade*****	02/17/2025	id theft forum
varun@tel5.com.au	Ade*****	12/17/2024	id theft forum
nick@tel5.com.au	003***** ***** ***** *****	09/28/2024	id theft forum
sarah@tel5.com.au	003***** ***** ***** ***** *****	09/28/2024	id theft forum
info@tel5.com.au		03/24/2024	id theft forum