isse

SECURITY. ENGINEERED.

COMPANY SECURITY REVIEW

Ziemeļu birojs.
A clear view of security.

SIA ZIEMEĻU BIROJS · DEMONSTRATION COMPANY

A limited-scope professional review. All company data and findings in this document are fictional.

VERSIJA 1.0 · 2026-11-15 · info@isse.lv

08 PAGES

DEMONSTRATION · NOT A REAL CLIENT REPORT

02 · MANAGEMENT SUMMARY

The priorities are clear.

2
HIGH PRIORITY

4
RECOMMENDED IMPROVEMENTS

8
WITHOUT IDENTIFIED ISSUE

MOST IMPORTANT NEXT STEPS

ISSE-001 **Incomplete multifactor authentication coverage**

Enable MFA for every user, starting with email and remote access. Permit exceptions only for a time-bound, documented reason.

ISSE-002 **Former-employee access requires a further review**

Review active sessions, groups, shared resources, VPN, the password manager and physical access. Document the completed actions.

ISSE-003 **DMARC is configured for monitoring only**

Review DMARC reports and every legitimate sender. After verification, move gradually to p=quarantine or p=reject.

CONTROLS WITHOUT AN IDENTIFIED ISSUE

- The number of administrator accounts is limited and daily accounts are not used for administration.
- A password manager is in use and the IT provider has a shared-access register.
- An SPF record is present and there are no conflicting multiple records.
- DKIM signing is used for at least the primary Microsoft 365 mail flow.
- Employee access groups have a named owner.
- Operating-system updates on work devices are centrally monitored.

This is not a single security percentage. The result reflects only the agreed scope and available evidence.

03 · ASSESSMENT SCOPE

What was and was not checked.

The review provides a clear, usable first view; it does not certify comprehensive compliance or security.

TECHNICALLY CHECKED	Public DNS records, DMARC policy and the demonstration Microsoft 365 configuration extract.
CLIENT-SUPPLIED INFORMATION	Employee count, processes, device management, access revocation and backup practice.
NOT VERIFIED	Every device, client-data content, internal servers, message delivery and actual user experience.
NOT APPLICABLE	Controls without a matching object in the demonstration environment or outside the agreed scope.

LIMITATIONS

- A time-limited remote review with a 90-minute target scope.
- No full audit, penetration test, inspection of every device or regulatory certification.
- The report reflects a specific point in time; environments and threats change.
- Missing evidence means “not verified”, not automatically “insecure”.

04 · FINDINGS AND RECOMMENDATIONS

What needs attention and why.

ISSE-001

TECHNICALLY CHECKED · IMMEDIATELY

Incomplete multifactor authentication coverage

IDENTITY AND ACCOUNT SECURITY · HIGH

OBSERVATION

In the demonstration dataset MFA is enabled for administrators, but not every email and remote-access user. At least two user accounts still rely on one factor.

RECOMMENDATION

Enable MFA for every user, starting with email and remote access. Permit exceptions only for a time-bound, documented reason.

IMPACT

One stolen password could provide access to a mailbox or remote environment. This may expose client data, enable fraudulent messages and lead to fake payment requests.

TECHNICAL DETAIL

Review Microsoft Entra authentication methods and the enterprise-access policy. Confirm that legacy authentication is not available as a practical bypass.

OWNER: IT provider with business owner approval

ISSE-002

CLIENT-SUPPLIED INFORMATION · IMMEDIATELY

Former-employee access requires a further review

ACCESS MANAGEMENT · HIGH

OBSERVATION

The client environment description says an employee left six weeks ago. Email was blocked, but revocation of shared folders and password-manager access is not documented.

RECOMMENDATION

Review active sessions, groups, shared resources, VPN, the password manager and physical access. Document the completed actions.

IMPACT

Unrevoked access can remain invisible and create confidentiality or data-integrity risk.

TECHNICAL DETAIL

Compare the user's direct and group permissions with an approved access matrix. Review OneDrive and SharePoint external sharing links.

OWNER: IT provider and HR

ISSE-003

TECHNICALLY CHECKED · WITHIN 7 DAYS

DMARC is configured for monitoring only

EMAIL SECURITY · MEDIUM

OBSERVATION

Public DNS has one DMARC record with p=none. SPF and DKIM are configured in the demonstration data, but were not verified through actual message authentication.

RECOMMENDATION

Review DMARC reports and every legitimate sender. After verification, move gradually to p=quarantine or p=reject.

IMPACT

Monitoring policy provides visibility but does not itself stop messages spoofing the domain in user inboxes.

TECHNICAL DETAIL

Include CRM, invoicing, website contact forms and other senders. Verify SPF and DKIM alignment before changing policy.

OWNER: IT provider

05 · FINDINGS AND RECOMMENDATIONS

What needs attention and why.

ISSE-004 — CLIENT-SUPPLIED INFORMATION · WITHIN 30 DAYS

Data restoration testing is not documented

BACKUPS · MEDIUM

OBSERVATION

Client-supplied information confirms automatic Microsoft 365 and device backup. There is no evidence of a real restoration test for at least one file or a recorded recovery time.

RECOMMENDATION

Perform a controlled restoration to a separate location, verify the content and record actual duration, issues and the next test date.

IMPACT

Backup status alone does not show whether data can be restored in an acceptable time or whether a compromised administrator can delete the copies.

TECHNICAL DETAIL

Review immutable retention, a separate access model and deletion protection from administrative rights.

OWNER: IT provider with the business owner

ISSE-005 — CLIENT-SUPPLIED INFORMATION · WITHIN 30 DAYS

Disk-encryption status is not consistently verified

WORK DEVICES · MEDIUM

OBSERVATION

Encryption is described as enabled on Windows devices, but FileVault status and recovery-key management on macOS devices are not confirmed.

RECOMMENDATION

Check every laptop regardless of operating system and centralise recovery-key management.

IMPACT

A lost unencrypted device may expose client files and saved sign-in data.

TECHNICAL DETAIL

Confirm FileVault and BitLocker status is monitored by a management solution, not only visible on the user's screen.

OWNER: IT provider

ISSE-006 — CLIENT-SUPPLIED INFORMATION · WITHIN 90 DAYS

Security guidance for employees is not documented

EMPLOYEE AWARENESS · LOW

OBSERVATION

New employees receive an oral explanation of sign-in and data storage. There is no common material or record that guidance was received.

RECOMMENDATION

Create a short practical resource, include it in onboarding and repeat the main scenarios at least annually.

IMPACT

Different understanding of suspicious email and payment verification may increase fake-invoice and accidental-sharing risk.

TECHNICAL DETAIL

State the reporting mailbox or IT contact and verify that a test message is noticed and handled promptly.

OWNER: Management with the IT provider

06 · ACTION PLAN

A sequence that can be delivered.

Some actions can be completed by the business or existing IT provider. Others may require a clear technical decision or external help.

IMMEDIATELY

ISSE-001 · Complete MFA coverage for email and remote access.
ISSE-002 · Revoke all remaining former-employee sessions and access.

WITHIN 7 DAYS

ISSE-003 · Review DMARC reports and confirm legitimate senders.
Test the user-support process after MFA rollout.

WITHIN 30 DAYS

ISSE-004 · Perform and document the first restoration test.
ISSE-005 · Centralise BitLocker and FileVault status and key management.

WITHIN 90 DAYS

ISSE-006 · Introduce practical employee security guidance.
Re-review open findings and the access matrix.

DEPENDENCIES AND REVIEW

After MFA rollout, verify the user-support process. Complete the sender inventory before tightening DMARC. Before the restoration test, confirm who may access backups and who approves the result.

07 · OPTIONAL IMPLEMENTATION

Help is a choice, not a condition.

Prices are confirmed only after reviewing the scope and environment. These steps are not a binding offer and require a separate written agreement.

01

MFA and account-access setup

Price confirmed after scope review

Authentication-method review, MFA coverage, administrator-account review and short change documentation.

Approx. 3-4 hours

An additional licence may be required depending on the chosen method.

02

Email authentication improvement

Price confirmed after scope review

Sender review, SPF and DKIM corrections, DMARC monitoring review and a plan for stronger policy.

Approx. 3-5 hours

Normally no additional licence.

03

Backup restoration workshop

Price confirmed after scope review

One controlled restoration test, results documentation, gap list and creation of the next test process.

Approx. 3-4 hours

Depends on the existing backup solution.

The existing IT provider may complete any recommendation where it has the required access and competence. ISSE involvement is not required for the action plan to be usable.

08 · NEXT STEPS

The decisions remain yours.

The report is intended for a conversation with management and the IT provider. Priorities may be adjusted for actual impact, available help and environment dependencies.

NEXT STEPS

- Confirm ownership for the two high-priority actions.
- Agree the DMARC sender inventory.
- Schedule a tested data restoration.
- Re-review open findings after 90 days.

LIMITATIONS

- Not a full audit or penetration test.
- Not a compliance certification.
- Not a review of every device or client-data store.
- The report reflects a specific point in time.

CONFIDENTIALITY

A real client report must use only approved data, restricted access and a separate private data environment. This public sample contains no client evidence or sign-in information.

USEFUL RESOURCES

isse.lv/free-tools · isse.lv/knowledge

info@isse.lv · +371 24 421 133