SAMPLE REPORT

Brokerage Cybersecurity Assessment

Prepared for: Pinecrest Realty Group

Assessment Date:	June 2026
Report Date:	June 2026
Prepared by:	Real Estate Cyber Trust
Operated by:	Ironvon Inc. · Ontario Business Registry
Assessor:	S. Devarajah, CISSP #624284 · Ontario Licensed Realtor
Classification:	CONFIDENTIAL — Client Use Only

OVERALL RISK RATING	HIGH	Three areas require prompt attention. Wire transfer and email security are the highest-priority findings.

SECTION 1

Executive Summary

Real Estate Cyber Trust conducted a remote cybersecurity assessment of Pinecrest Realty Group during June 2026. The assessment evaluated five key areas: email security, MLS and PropTx access controls, client personal information handling, wire transfer process security, and public-facing exposure. The assessment was conducted via structured intake questionnaire and observable technical signals; no system access or software installation was required.

Pinecrest Realty Group is a 22-agent brokerage operating from a single Mississauga office. Deal files are managed through a shared Google Drive, agent email runs on individual Gmail accounts (not a brokerage domain), and wire transfer instructions are communicated via unencrypted email. These conditions represent the most common attack surface exploited in Ontario real estate fraud cases.

Assessment Area Summary

Assessment Area	Risk Level	Key Finding
Email Security	HIGH	No brokerage domain; agents on personal Gmail. No DMARC.
MLS / PropTx Access	MEDIUM	Shared credentials in use; no offboarding procedure documented.
Client PII Handling	HIGH	Deal files on personal Google Drives; no access controls.
Wire Transfer Process	HIGH	Instructions sent via unencrypted email; no callback verification.
Public-Facing Exposure	LOW	Website does not collect personal data. No exposed admin panels.

Immediate Priority Actions

- Migrate all agent email to a brokerage-owned domain (e.g. @pinecrestrealty.ca) with DMARC enforcement.
- Implement a documented wire transfer verification procedure: callback to a known phone number before any deposit redirection.
- Replace shared Google Drive with access-controlled document management; remove personal Drive usage for deal files.
- Establish and document a PropTx credential offboarding process triggered on agent departure.

SECTION 2

Email Security

Risk Level **HIGH**

Findings

- Agents operate on personal Gmail accounts (e.g. agentname@gmail.com) with no brokerage domain.
- The brokerage domain pinecrestrealty.ca has no SPF, DKIM, or DMARC DNS records configured, leaving it open to spoofing.
- No phishing awareness training documented for agents in the past 12 months.
- Email is used as the primary channel for communicating deposit instructions, purchase conditions, and client personal information.

Recommendations

- Register a brokerage email domain and migrate all agents to brokerage-managed accounts (Google Workspace or Microsoft 365 are both suitable).
- Configure SPF, DKIM, and DMARC on the brokerage domain. DMARC policy should be set to 'reject' once validated.
- Conduct annual phishing awareness training. ESET, KnowBe4, and Proofpoint all offer small-business packages.
- Establish a written policy that deposit and wire instructions are never communicated or modified solely by email.

SECTION 3

MLS / PropTx Access Controls

Risk Level **MEDIUM**

Findings

- Two agents confirmed sharing a single PropTx login for administrative tasks.
- No documented offboarding checklist; a former agent's credential was active for an estimated 3 weeks post-departure.
- PropTx password last reset over 14 months ago for 7 of 22 accounts reviewed.
- No multi-factor authentication enforced at the brokerage level on PropTx accounts.

Recommendations

- Enforce individual PropTx credentials for every agent. Shared logins eliminate audit trail and violate PropTx Terms of Service.
- Create a written offboarding procedure: PropTx deactivation within 24 hours of an agent's departure.
- Set a 90-day forced password rotation policy for all PropTx accounts.
- Enable MFA on PropTx wherever available; monitor ITSO/PropTx release notes for MFA mandate updates.

SECTION 4

Client Personal Information Handling

Risk Level **HIGH**

Findings

- Deal files containing SINs, financial statements, and signed OREA forms are stored in individual agents' personal Google Drive accounts — not a brokerage-controlled system.
- No documented data retention or destruction policy for client files post-closing.
- Client intake forms collected verbally or via unencrypted email; no secure intake process documented.
- No PIPEDA breach response procedure in place; broker of record was unaware of mandatory 72-hour OPC breach notification requirement.

Recommendations

- Migrate all deal files to a brokerage-controlled document management system (Skyslope, Brokermint, or a controlled Google Workspace shared drive with permission management).
- Draft and implement a data retention policy: retain deal files for 7 years per CRA requirements, then securely destroy.
- Implement a secure intake process for client personal data — encrypted web form or in-person only for SIN collection.
- Brief the broker of record on PIPEDA breach notification obligations. Designate a privacy officer (can be the broker of record in a small brokerage).

SECTION 5

Wire Transfer Process Security

Risk Level **HIGH**

Findings

- Deposit and closing fund instructions are communicated entirely via email with no secondary verification step.
- No written wire transfer policy exists; agents handle deposit redirection requests independently.
- Three agents surveyed were unaware of Business Email Compromise (BEC) as an attack vector.
- The brokerage has not subscribed to any real estate fraud alerts (RECO, OREA, or bank-issued).

Recommendations

- Implement a mandatory callback verification rule: any request to change deposit destination must be verbally verified by phone to a known number before acting.
- Publish and enforce a one-page Wire Transfer Security Policy signed by all agents annually.
- Brief all agents on BEC attack patterns specific to real estate; RECO has published guidance materials available at reco.on.ca.
- Subscribe to OREA fraud alerts and ensure the broker of record reviews them quarterly.

SECTION 6

Public-Facing Exposure

Risk Level LOW

Findings

- The brokerage website (pinecrestrealty.ca) does not collect personal data or run contact forms that transmit PII.
- No exposed admin panels, login pages, or staging environments found at the brokerage domain.
- SSL/TLS certificate is valid and correctly configured; HTTPS enforced.
- One outdated WordPress plugin (Contact Form 7, version 3 versions behind current) identified — low severity given no form usage.

Recommendations

- Update Contact Form 7 plugin to current version; enable automatic plugin updates or schedule monthly review.
- If a contact form is added to the site in future, ensure any PII collected is transmitted encrypted and stored in a brokerage-controlled system, not emailed to a personal Gmail.
- No urgent action required in this area. Re-assess if website functionality expands.

SECTION 7

Remediation Roadmap

The following prioritized roadmap is recommended based on risk level and implementation effort. Items are grouped by timeline — not all require external vendors or significant cost.

Timeline	Action	Area	Effort
Immediate (0–2 weeks)	Implement callback verification for all wire/deposit changes	Wire Transfer	Low
Immediate (0–2 weeks)	Remove shared PropTx credential; issue individual accounts	MLS Access	Low
30 days	Migrate brokerage to domain email (Google Workspace or M365)	Email	Medium
30 days	Configure SPF, DKIM, DMARC on brokerage domain	Email	Low
30 days	Deactivate departed agent PropTx credentials; document procedure	MLS Access	Low
60 days	Migrate deal files to brokerage-controlled document system	Client PII	Medium
60 days	Brief broker of record on PIPEDA breach notification obligations	Client PII	Low
90 days	Conduct BEC / wire fraud awareness session for all agents	Wire Transfer	Low
90 days	Publish signed Wire Transfer Security Policy	Wire Transfer	Low
Ongoing	Annual phishing training; PropTx password rotation every 90 days	Email / MLS	Low

APPENDIX

About This Assessment

This assessment was conducted by Real Estate Cyber Trust, operated by Ironvon Inc., an Ontario incorporated company. The assessor holds CISSP certification (ISC2 #624284) and an active Ontario real estate licence. The combination of cybersecurity credentials and real estate industry experience allows for assessment of risks specific to Ontario brokerage operations, including PropTx/MLS workflows, OREA transaction processes, and the regulatory context under RECO and PIPEDA.

Scope and Methodology

This assessment was conducted remotely using: (1) a structured intake questionnaire completed by the broker of record and designated administrative contact; (2) observable technical signals including DNS record inspection, SSL/TLS configuration review, and public-facing website analysis; and (3) review of any policy documentation provided during intake. No system access, network credentials, or software installation was required or used.

Limitations

This assessment represents a point-in-time review based on information available and provided during the assessment period. It does not constitute a penetration test, vulnerability scan, or audit under any regulatory framework. Findings reflect the information provided in intake; material omissions or changes in the brokerage's environment after the assessment date may affect conclusions. This report does not constitute legal advice, and does not certify compliance with any legislation, regulation, or standard.

Confidentiality

This report is prepared exclusively for Pinecrest Realty Group and Ironvon Inc. It is classified CONFIDENTIAL and may not be shared, published, or reproduced in whole or in part without written consent from Ironvon Inc. Intake data collected during this engagement is retained only for the duration of the engagement and is handled in accordance with PIPEDA.

Real Estate Cyber Trust Operated by Ironvon Inc.	realestatecybertrust.ca	CISSP #624284 Ontario Real Estate Licence Active