

Acceptable Use Policy

Last Revised: July 10, 2026

1. Introduction

This Acceptable Use Policy ("Policy") governs the use of websites, client accounts, hosted services, electronic signature tools, file storage, support systems, application programming interfaces, and other services operated or provided by Huronia Systems Ltd. ("Huronia Systems", "we", "us", or "our").

This Policy forms part of the Huronia Systems Terms & Conditions.

By accessing or using the Services, you agree to comply with this Policy and all applicable laws, regulations, Project Agreements, and service-specific requirements.

Where a signed Project Agreement contains terms that conflict with this Policy, the signed Project Agreement will prevail to the extent of the conflict.

2. Scope

This Policy applies to all persons who access or use the Services, including Clients, authorized users, account administrators, contractors, employees of Clients, and visitors.

The Services covered by this Policy may include:

- The Huronia Systems website;
- The Client Portal;
- Client accounts;
- Electronic signature services;
- File upload and download features;
- Support and ticketing systems;
- Hosted websites and applications;
- Managed infrastructure;
- Application programming interfaces;
- Administrative dashboards;
- Knowledge bases;
- Communication tools; and

- Other systems made available by Huronia Systems.

This Policy applies whether the Services are accessed directly, through an integration, through an automated system, or through another person acting on your behalf.

3. General Use Requirements

You must use the Services responsibly, lawfully, and only for their intended purposes.

You are responsible for:

- Ensuring that your use of the Services complies with applicable law;
- Maintaining accurate account and contact information;
- Protecting your login credentials and access methods;
- Ensuring that persons using your account are authorized;
- Maintaining appropriate backups of information under your control;
- Obtaining all permissions required for content you upload or process;
- Following reasonable instructions provided by Huronia Systems; and
- Cooperating with investigations involving suspected misuse or security incidents.

You must not use the Services in a manner that could harm Huronia Systems, another Client, a third party, or the security, availability, integrity, or reputation of the Services.

4. Prohibited Unlawful Activity

You must not use the Services to engage in, promote, facilitate, or support unlawful activity.

Prohibited activity includes:

- Fraud or attempted fraud;
- Identity theft or impersonation;
- Unauthorized access to systems, accounts, or information;
- Distribution of stolen or unlawfully obtained information;
- Infringement of intellectual property rights;
- Harassment, threats, stalking, or intimidation;
- Defamation or unlawful publication of private information;
- Distribution of illegal goods, services, or content;
- Evasion of sanctions, court orders, or legal restrictions;
- Violation of privacy, consumer protection, or anti-spam laws; or

- Any activity that exposes Huronia Systems to legal or regulatory liability.

Huronia Systems may refuse, suspend, or terminate Services where it reasonably believes that the Services are being used for unlawful purposes.

5. Security and System Integrity

You must not interfere with or attempt to compromise the security, integrity, availability, or operation of the Services.

Prohibited conduct includes:

- Introducing malware, ransomware, viruses, spyware, or harmful code;
- Attempting to bypass authentication or access controls;
- Accessing another person's account without authorization;
- Scanning, probing, or testing systems for vulnerabilities without written authorization;
- Exploiting or attempting to exploit a security vulnerability;
- Interfering with network traffic, servers, databases, or applications;
- Conducting denial-of-service or distributed denial-of-service attacks;
- Circumventing usage limits, rate limits, or technical restrictions;
- Concealing the source or destination of malicious activity;
- Using automated tools in a manner that creates unreasonable system load;
- Attempting to extract credentials, tokens, keys, or protected information; or
- Assisting another person in carrying out prohibited security activity.

You must promptly notify Huronia Systems if you become aware of:

- Unauthorized account access;
- Exposed credentials;
- A suspected vulnerability;
- Loss of a device containing access information;
- Malicious files uploaded through the Services; or
- Any other security incident affecting the Services.

Security concerns may be reported to info@huroniasystems.ca.

6. Account and Access Restrictions

You must not:

- Share an account with unauthorized persons;
- Create accounts using false or misleading information;
- Use another person's identity or contact information without permission;
- Allow a suspended or terminated user to access the Services through your account;
- Sell, transfer, lease, or sublicense access to an account without authorization;
- Attempt to access administrative functions not made available to you;
- Use credentials obtained through deception, theft, or technical exploitation; or
- Continue accessing the Services after authorization has been withdrawn.

You are responsible for activity performed through your account by persons you have authorized.

Huronia Systems may require password resets, additional identity verification, or temporary access restrictions where reasonably necessary to protect an account or the Services.

7. Content and File Uploads

You must not upload, store, transmit, publish, or make available through the Services any content that:

- Is unlawful, fraudulent, deceptive, defamatory, threatening, abusive, or harassing;
- Infringes copyright, trademark, privacy, contractual, or other legal rights;
- Contains malware, malicious scripts, corrupted files, or harmful code;
- Contains personal information that you are not authorized to collect, use, or disclose;
- Is intended to mislead others about its source, identity, or authenticity;
- Promotes violence, discrimination, exploitation, or other unlawful conduct;
- Violates confidentiality obligations;
- Is subject to legal restrictions that prohibit its storage or transmission; or
- Creates an unreasonable legal, security, or operational risk for Huronia Systems.

You are responsible for all content uploaded or submitted through your account.

Huronia Systems may remove, restrict, quarantine, or disable access to content where reasonably necessary to protect the Services, comply with legal obligations, or investigate suspected misuse.

8. Electronic Signatures and Documents

You must use electronic signature tools only for legitimate and authorized purposes.

You must not:

- Sign on behalf of another person without authority;
- Falsify, alter, or misrepresent a signature record;
- Attempt to manipulate timestamps, IP records, device information, or audit data;
- Submit a document under a false identity;
- Interfere with the integrity of a signed document;
- Reuse a signature for a purpose not authorized by the signer; or
- Use the electronic signature system to facilitate fraud or unlawful activity.

You are responsible for confirming that you have authority to sign and that the information contained in the document is accurate before submitting an electronic signature.

Huronia Systems may preserve audit records associated with electronic signatures for verification, security, contractual, and legal purposes.

9. Support and Communication Tools

Support tickets, forms, messaging tools, email, SMS, and other communication features must be used respectfully and for legitimate business purposes.

You must not use these tools to:

- Harass, threaten, intimidate, or abuse another person;
- Submit knowingly false or misleading complaints;
- Send excessive, repetitive, or disruptive messages;
- Transmit malicious links or attachments;
- Impersonate another person or organization;
- Submit confidential information that you are not authorized to disclose;
- Attempt to manipulate support staff into bypassing security controls; or
- Use support channels for unsolicited advertising or solicitation.

Huronia Systems may restrict access to support or communication features where they are used abusively or in a manner that interferes with normal operations.

10. Hosted Services and Infrastructure

Where Huronia Systems provides hosting, infrastructure management, or related technical services, you must not use those Services to:

- Host unlawful content or services;
- Operate phishing, credential theft, or malware distribution systems;
- Send unsolicited commercial messages;
- Conduct unauthorized scanning, intrusion attempts, or attacks;
- Operate services designed to conceal unlawful activity;
- Mine cryptocurrency without prior written authorization;
- Consume excessive resources in a manner that materially affects other users or systems;
- Circumvent storage, bandwidth, or usage restrictions;
- Resell or sublicense hosting without written authorization; or
- Operate a service that creates an unreasonable risk to network reputation or availability.

Huronia Systems may apply reasonable technical restrictions, rate limits, storage limits, traffic controls, or other measures to protect hosted systems and infrastructure.

11. APIs, Automation, and Automated Access

You must not use APIs, scripts, bots, crawlers, or automated tools to:

- Circumvent authentication, rate limits, or access controls;
- Extract information not intended for automated access;
- Create unreasonable traffic or system load;
- Attempt to discover protected endpoints or vulnerabilities;
- Scrape personal information without authorization;
- Replicate or resell the Services without written permission;
- Automate fraudulent, abusive, or deceptive activity; or
- Interfere with the normal use of the Services by others.

Huronia Systems may restrict, throttle, suspend, or revoke automated access where reasonably necessary to protect the Services.

Any API access may also be subject to additional technical requirements, usage limits, or service-specific terms.

12. Intellectual Property and Reverse Engineering

You must not:

- Copy, reproduce, distribute, sell, or exploit Huronia Systems' materials without authorization;
- Remove copyright notices, watermarks, branding, or access restrictions;
- Reverse engineer, decompile, disassemble, or attempt to derive source code from protected software or preview materials;
- Copy the structure, design, workflow, or proprietary elements of the Client Portal or other Services;
- Use Huronia Systems' trademarks, logos, or branding without authorization;
- Provide preview materials to another developer for replication; or
- Use internal documentation, credentials, or administrative information outside the purpose for which they were provided.

Nothing in this Policy grants ownership or licence rights except where expressly stated in writing.

13. Resource Usage and Service Stability

You must not use the Services in a manner that causes excessive, abnormal, or disruptive consumption of:

- Processing capacity;
- Memory;
- Storage;
- Bandwidth;
- Database resources;
- Email delivery capacity;
- API requests; or
- Support resources.

Huron Systems may investigate abnormal usage and may require corrective action.

Where usage materially affects service stability, security, cost, or other users, Huronia Systems may impose reasonable limits, suspend affected features, or require a different service arrangement.

14. Monitoring and Enforcement

Huron Systems may monitor the Services to the extent reasonably necessary to:

- Maintain security and availability;
- Investigate suspected misuse;
- Enforce this Policy and the Terms & Conditions;
- Comply with legal obligations;
- Diagnose technical issues; and
- Protect Huronia Systems, its Clients, users, and third parties.

Monitoring may include reviewing account activity, logs, uploaded content, traffic patterns, support records, and security events where reasonably necessary.

Huron Systems does not undertake a general obligation to monitor all activity or content.

Where a violation is suspected or confirmed, Huronia Systems may:

- Issue a warning;
- Require corrective action;
- Remove or restrict content;
- Reset credentials;
- Limit functionality;
- Suspend an account or Service;
- Terminate access;
- Preserve relevant records;
- Notify affected parties;
- Report unlawful conduct to appropriate authorities; or
- Take other reasonable action necessary to protect the Services.

15. Reporting Violations

Suspected violations of this Policy may be reported to:

Huroniasystems Ltd.

Email: info@huroniasystems.ca

Telephone: (705) 321-1035

Reports should include enough information to identify the affected account, content, or activity and explain the basis for the concern.

Huroniasystems may request additional information where reasonably necessary to investigate a report.

Knowingly false, abusive, or misleading reports may themselves constitute a violation of this Policy.

16. Changes to this Policy

Huroniasystems may update this Policy to reflect changes to the Services, technologies, operational practices, or legal obligations.

The current version will be identified by the "Last Revised" date at the beginning of this Policy.

Material changes may be communicated through the website, Client Portal, email, or another reasonable method.

Continued use of the Services after an updated Policy takes effect constitutes acceptance of the revised Policy, except where additional consent is required by law.