decision digital

Acceptable Use Policy

decisiondigital.com

6105 Blue Stone Road, Suite F
Atlanta, GA 30328 | 404.303.0330

Acceptable Use Policy

Effective Date: October 1997 | Last Updated: April 2025

1. PURPOSE AND SCOPE

This Acceptable Use Policy ("AUP") governs the use of all services, platforms, systems, networks, software, and infrastructure provided by Decision Digital, Inc. ("Provider," "we," "us," or "our") under any Managed Services Agreement ("MSA"), Service Attachment, Statement of Work, or Order (collectively, the "Agreement"). This AUP applies to all clients ("Client," "you"), their employees, contractors, authorized users, and any third parties who access or use the Services through Client's accounts or credentials.

This AUP is incorporated by reference into the Agreement and into all Service Attachments executed between the parties. In the event of a conflict between this AUP and any Service Attachment with respect to acceptable use, the Service Attachment shall control for the specific services it governs. In all other respects, this AUP shall control.

Provider reserves the right to modify this AUP at any time. Updated versions will be published at https://www.decisiondigital.com/doc-aup/ and will become effective upon posting. Provider will notify Client of material changes within thirty (30) days of any update that materially restricts Client's use of the Services.

2. PROHIBITED USES

Client shall not use the Services, and shall ensure that its employees, contractors, and authorized users do not use the Services, for any of the following purposes:

2.1 Illegal and Harmful Activity

- Engaging in any activity that violates applicable federal, state, local, or international law or regulation, including but not limited to the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the CAN-SPAM Act, HIPAA, GDPR, or any applicable state data protection laws.
- Transmitting, storing, or processing any content that constitutes, facilitates, or promotes illegal activity of any kind.

- Engaging in harassment, stalking, threats, abuse, or discrimination against any individual or group.
- Violating the intellectual property rights, privacy rights, or other legal rights of any person or entity.

2.2 Security Violations

- Attempting to gain unauthorized access to any system, network, account, data, or resource, whether belonging to Provider, Client, or any third party.
- Introducing, transmitting, or storing malware, ransomware, viruses, trojans, worms, spyware, adware, or any other malicious code.
- Conducting or facilitating any denial-of-service (DoS) or distributed denial-of-service (DDoS) attack against any system or network.
- Intercepting, monitoring, or capturing network traffic or communications without proper authorization.
- Exploiting or attempting to exploit any vulnerability in any system, application, or network.
- Using the Services to conduct penetration testing, vulnerability scanning, or security assessments on any systems other than Client's own, without prior written authorization from Provider.

2.3 Credential and Access Misuse

- Sharing, transferring, or disclosing user credentials, access keys, API keys, tokens, or passwords to any unauthorized person or third party.
- Using another person's credentials to access the Services without authorization.
- Creating or using unauthorized accounts or credentials to access the Services.
- Allowing credentials to remain active for terminated employees, contractors, or other former authorized users. Client is responsible for promptly notifying Provider of any personnel changes requiring credential revocation.
- Bypassing or attempting to bypass any authentication, access control, or security mechanism implemented by Provider.

2.4 Data and Privacy Violations

- Processing, storing, or transmitting personal data in violation of applicable privacy laws, including without limitation HIPAA, GDPR, CCPA, or any other applicable data protection regulation.
- Collecting, harvesting, or aggregating personal information from the Services or from third parties without proper legal basis and appropriate disclosures.
- Transmitting or storing any data that is subject to heightened regulatory protection — including protected health information (PHI), payment card data (PCI), classified government information, or export-controlled data — without prior written authorization from Provider and appropriate safeguards in place.
- Using the Services in a manner that would expose Provider to liability under any privacy law or regulation applicable to Client's data or industry.

2.5 Network and Resource Abuse

- Consuming network bandwidth, storage, computing resources, or other shared infrastructure in a manner that materially degrades the Services for other users or that exceeds agreed resource allocations.
- Using the Services to mine cryptocurrency or perform other computationally intensive tasks not related to the contracted Services without prior written consent from Provider.
- Sending unsolicited bulk communications (spam) or any communication that violates the CAN-SPAM Act or equivalent regulations.
- Using the Services to operate open mail relays, proxy servers, or other intermediary services that could be used to obscure the origin of malicious activity.

2.6 Intellectual Property and Content

- Reproducing, distributing, publicly displaying, or creating derivative works from any Provider Materials, third-party materials, or other proprietary content without authorization.
- Removing, altering, or obscuring any copyright, trademark, or other proprietary rights notices from Provider Materials or third-party materials.

- Transmitting or storing any content that infringes any patent, trademark, trade secret, copyright, or other intellectual property right.
- Reverse engineering, decompiling, disassembling, or otherwise attempting to derive the source code of any Provider software, platform, or tool.

2.7 High-Risk Use

- Using the Services in any application where failure could lead to death, serious bodily injury, or severe physical or environmental damage, including but not limited to life support systems, nuclear facilities, aircraft navigation, or emergency response systems, without prior written consent from Provider and appropriate redundancy measures in place.

3. CLIENT RESPONSIBILITIES

Client accepts full responsibility for all use of the Services by its employees, contractors, authorized users, and any third parties who access the Services through Client's accounts or credentials, whether or not such use was authorized by Client.

3.1 Security Obligations

- Maintain current, supported, and properly licensed security software on all systems connected to or accessing the Services, including antivirus, anti-malware, and endpoint protection.
- Implement and enforce multi-factor authentication (MFA) on all accounts and credentials used to access the Services, where technically supported.
- Promptly apply all security patches, updates, and firmware upgrades recommended by Provider within commercially reasonable timeframes.
- Reboot devices promptly when directed by Provider to complete the application of security updates or patches. Provider shall bear no liability for security exposure resulting from Client's failure to reboot as directed.
- Maintain current cyber liability insurance coverage as required under the Agreement and TOS.

3.2 Personnel Management

- Promptly notify Provider of any employee, contractor, or authorized user termination or role change requiring credential revocation or access modification. Provider's standard processing time for access revocation is one (1) business day following receipt of written notice.
- Ensure that all authorized users are aware of and trained on this AUP and applicable security policies.
- Promptly report any suspected unauthorized access, security incident, or AUP violation to Provider.

3.3 Compliance Obligations

- Maintain compliance with all applicable laws, regulations, and industry standards governing Client's use of the Services and the data processed through the Services.
- Obtain all necessary consents, authorizations, and licenses required for Client's use of the Services, including any third-party software licenses.
- Cooperate fully with Provider's reasonable requests related to compliance investigations, security incidents, or AUP enforcement.

4. ACKNOWLEDGMENT OF DECLINED RECOMMENDATIONS

If Client declines, defers, or fails to act upon any security, configuration, or operational recommendation made by Provider, Provider may document such declination in writing via email, ticketing system, or other written communication. Client's failure to object to Provider's written documentation of a declined recommendation within five (5) business days shall constitute Client's acknowledgment of such declination. Provider's liability for any damages arising from or related to a declined recommendation shall be fully extinguished upon such documentation.

Client acknowledges that failure to implement Provider's security recommendations — including but not limited to patch management, MFA enforcement, credential hygiene, and backup compliance — may result in increased security risk and that Provider shall bear no liability for any resulting incidents or damages.

5. ENFORCEMENT AND REMEDIES

5.1 Monitoring

Provider reserves the right to monitor use of the Services to the extent permitted by applicable law and the Agreement for the purpose of ensuring compliance with this AUP, maintaining the security and integrity of the Services, and investigating suspected violations.

5.2 Suspension

Provider may immediately suspend access to all or any portion of the Services, without prior notice to Client, if Provider reasonably believes that:

- Client or any authorized user is engaged in activity that violates this AUP;
- The Services are being used in a manner that poses a security risk to Provider, Client, other clients, or third parties;
- Client's use of the Services is causing or is likely to cause legal liability for Provider; or
- Client is in material breach of the Agreement.

Provider will use commercially reasonable efforts to notify Client as soon as practicable following any suspension. Suspension does not relieve Client of its payment obligations under the Agreement.

5.3 Termination

Provider may terminate the Agreement in accordance with its termination provisions upon Client's material or repeated violation of this AUP. Termination for AUP violation shall not relieve Client of any termination fee obligations under the Agreement unless the violation constitutes grounds for termination with cause, in which case the applicable with-cause termination provisions of the Agreement shall govern.

5.4 Legal Action

Provider reserves the right to cooperate with law enforcement and regulatory authorities and to pursue all available legal and equitable remedies against any person or entity that violates this AUP. Provider shall be entitled to seek injunctive relief, damages, and any other available remedies, including recovery of attorneys' fees, in connection with any material AUP violation.

6. CLIENT INDEMNIFICATION

Client shall indemnify, defend, and hold harmless Provider and its officers, directors, employees, agents, contractors, and subcontractors from and against any and all third-party claims, actions, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to:

- Client's violation of this AUP;
- Client's or any authorized user's unauthorized, improper, or illegal use of the Services;
- Any claim that Client's use of the Services infringes the intellectual property, privacy, or other rights of any third party;
- Any data breach, security incident, or unauthorized access arising from Client's failure to implement recommended security measures; or
- Any regulatory violation, fine, or penalty arising from Client's non-compliant use of the Services.

7. LIMITATION OF LIABILITY

NOTWITHSTANDING ANY OTHER PROVISION OF THIS AUP OR THE AGREEMENT, PROVIDER'S TOTAL CUMULATIVE LIABILITY ARISING FROM OR RELATED TO THIS AUP OR CLIENT'S USE OF THE SERVICES SHALL BE SUBJECT TO THE AGGREGATE LIABILITY CAP AND CONSEQUENTIAL DAMAGES WAIVER SET FORTH IN THE MSA. IN NO EVENT SHALL PROVIDER BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES ARISING

FROM CLIENT'S AUP VIOLATIONS OR MISUSE OF THE SERVICES, REGARDLESS OF WHETHER PROVIDER HAD NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

8. REPORTING VIOLATIONS

To report a suspected AUP violation, security incident, or unauthorized use of the Services, contact Provider at:

Decision Digital, Inc.

6105 Blue Stone Road, Suite F, Atlanta, GA 30328

Phone: 404.303.0330

Email: info@decisiondigital.com

Security incidents requiring immediate response should be reported by phone 24 hours per day, 7 days per week.

9. GOVERNING LAW AND RELATIONSHIP TO AGREEMENT

This AUP is governed by the laws of the State of Georgia, without regard to its conflicts of law principles. All disputes arising under this AUP shall be resolved in accordance with the dispute resolution provisions of the MSA, including the negotiation, arbitration, and jury waiver provisions set forth therein.

This AUP is incorporated into and forms part of the Agreement between Provider and Client. In the event of a conflict between this AUP and the MSA or any Service Attachment, the MSA or applicable Service Attachment shall control for matters within their respective scope. This AUP shall control for all matters relating to acceptable use of the Services not addressed in those documents.

Failure by Provider to enforce any provision of this AUP on any occasion shall not constitute a waiver of Provider's right to enforce that provision on any other occasion or to enforce any other provision of this AUP.

ACKNOWLEDGMENT

By executing the Managed Services Agreement, Client acknowledges that it has read, understood, and agrees to be bound by this Acceptable Use Policy. Client further acknowledges that this AUP may be updated from time to time and that continued use of the Services following notice of any update constitutes acceptance of the updated AUP.