# ACCEPTABLE USE POLICY - DOMANENNAME

Permitted and Prohibited Uses of Domains

Version: 1.0 Effective Date: 18th May 2026 Company: CRISALEO LIMITED Operating Domains: domanenname.com | domanenname.it | domanenname.eu | domanenname.us | domanenname.de

Governing Law: The laws of England and Wales \(English Law\) Jurisdiction: Courts of England and Wales

---

## 1. INTRODUCTION

This Acceptable Use Policy \("AUP"\) establishes the standards and requirements for use of domain names registered through Domanenname. All customers must comply with this policy and applicable laws.

This policy applies to:

- All domain registrations through Domanenname
- All websites hosted on registered domains
- All services accessed via registered domains
- All uses of domain nameservers and DNS configuration

Failure to comply may result in domain suspension, cancellation, and legal action.

---

## 2. PERMITTED USES

### 2.1 General Permitted Uses

Domains registered through Domanenname may be used for:

- Legitimate business operations \(websites, email, applications\)
- Personal use \(blog, portfolio, family site\)
- Non-profit purposes \(charities, community groups, educational\)
- Content and information sharing \(news, articles, educational) Tj ET BT /F1 1

- E-commerce and sales \(retail, services, digital goods\)
- Communication \(email, newsletters, customer service\)
- Parked domains \(held for future use, provided not used for abuse\)

### 2.2 Community and Social Purpose

Domains may be used for legitimate public benefit, including:

- Educational institutions and courses

- Open source software projects
- Community organisations and associations
- Journalism and news reporting
- Research and academic purposes
- Advocacy and public interest campaigns

### 2.3 Lawful Commercial Activities

Business and commercial uses are permitted, including:

- Sale of goods and services
- Professional services \(legal, medical, consulting\)
- Marketing and advertising \(with compliance to relevant) Tj ET BT /F1 11 Tf 1

- Affiliate marketing \(subject to disclosure requirements\)
- Subscription services and membership
- Marketplace and directory services

---

## 3. PROHIBITED USES

### 3.1 Illegal Activities

Domains MUST NOT be used for:

#### 3.1.1 Fraud and Deception

- Phishing: Domains impersonating legitimate services to steal credentials
- Fraudulent schemes: Advance-fee fraud, Ponzi schemes, pyramid schemes, fake investment schemes
- Identity theft: Using another person’s identity
- Financial fraud: Credit card fraud, wire fraud, cheque fraud
- Fake credentials: Falsely claiming professional qualifications, licenses, or authorizations
- Fake services: Impersonating government agencies, banks, or legitimate businesses
- Romance scams: Deceptive romantic relationships for financial gain

#### 3.1.2 Malware and Botnets

- Malware distribution: Hosting malware, viruses, trojans, spyware, ransomware
- Botnet command and control: Operating or hosting botnet infrastructure
- Exploit kits: Hosting tools or kits designed to compromise systems

- Cryptominers: Hosting or distributing software that hijacks computing resources
- Keyloggers and spyware: Distribution of data-stealing software

#### 3.1.3 Spam and Unsolicited Communications

- Email spam: Sending unsolicited bulk email \(SPAM\)
- Open relay abuse: Operating email servers for spam relay
- Spam distribution: Providing spam distribution services
- Comment spam: Automated posting of spam comments on blogs/forums
- SMS spam: Sending unsolicited text messages
- Telemarketing abuse: Illegal telemarketing calls or faxes

#### 3.1.4 Intellectual Property Violations

- Trademark counterfeiting: Selling counterfeit goods
- Trademark infringement: Using trademarked names to deceive \(cybersquatting\)
- Copyright infringement: Hosting infringing copyrighted content \(without license\)
- Piracy: Distribution of pirated software, films, music, games
- Plagiarism: Passing off others’ work as your own
- Trade secret theft: Misappropriation of confidential business information

#### 3.1.5 Exploitation of Minors

- Child exploitation material: Any content depicting child abuse
- Child sexual abuse material \(CSAM\): Strictly prohibited; reported to authorities
- Child grooming: Using domain to sexually exploit or manipulate minors
- Child sex trafficking: Using domain to facilitate trafficking
- Child endangerment: Any activity that endangers minors’ safety

#### 3.1.6 Illegal Drugs and Pharmaceuticals

- Drug trafficking: Sale or distribution of illegal drugs
- Prescription drug sales: Illegal sale of prescription medications without prescription
- Counterfeit pharmaceuticals: Selling fake medications
- Uncontrolled substance: Distribution of banned or controlled substances

#### 3.1.7 Weapons and Explosives

- Illegal weapons sales: Sale of weapons banned in relevant jurisdictions

- Explosives: Distribution of explosive materials or instructions
- Bomb-making: Hosting instructions for creating explosives or weapons
- Ammunition trafficking: Illegal ammunition sales

#### 3.1.8 Financial Crimes

- Money laundering: Facilitating illegal transfer of proceeds
- Tax evasion: Facilitating tax evasion or financial fraud
- Sanctions evasion: Circumventing international sanctions
- Terrorist financing: Facilitating funding of terrorist organisations
- Bribery: Soliciting or offering illegal payments

#### 3.1.9 Document Forgery and Fraud

- Forged documents: Creating or distributing forged credentials, licenses, passports
- Fake degrees: Selling fake educational credentials
- False certifications: Offering illegitimate professional certifications

### 3.2 Abuse and Harassment

Domains MUST NOT be used for:

#### 3.2.1 Harassment and Threats

- Harassment: Targeted harassment, bullying, or intimidation of individuals
- Threats and extortion: Death threats, threats of violence, extortion demands
- Doxxing: Publishing private personal information with intent to harass
- Defamation: Publishing false statements to damage reputation
- Stalking: Persistent unwanted contact or surveillance of individual
- Swatting: False emergency calls targeting specific individuals

#### 3.2.2 Hate Speech and Discrimination

- Hate speech: Content promoting hatred, violence, or discrimination based on:
  - Race or ethnicity
  - Religion
  - Gender or gender identity
  - Sexual orientation

  - Disability
  - Nationality
  - Age
  - Other protected characteristics
- Incitement to violence: Encouraging violence against protected groups
- Discrimination: Discriminatory services or content

#### 3.2.3 Harmful Content

- Suicide promotion: Hosting content promoting suicide or self-harm
- Eating disorder promotion: Promoting eating disorders or self-harm diets
- Violence promotion: Promoting or glorifying violence

### 3.3 Intellectual Property Infringement

Domains MUST NOT be used for:

#### 3.3.1 Copyright Infringement

- Pirated content: Hosting or distributing pirated films, TV, music, games
- Infringing replicas: Copies of copyrighted works without license
- Unauthorized mirrors: Mirroring copyrighted sites without permission
- Streaming piracy: Offering pirated streams of copyrighted content

#### 3.3.2 Trademark Violations

- Cybersquatting: Registering domains with famous trademarks with intent to profit or defraud
- Typosquatting: Similar domains intended to deceive users \(e.g.,) Tj ET BT /F1

- Trademark impersonation: Impersonating trademark holders
- Counterfeit goods: Selling counterfeit products branded with trademarks
- Brand confusion: Using similar branding to create confusion with legitimate businesses

#### 3.3.3 Patent Infringement

- Unauthorized use: Using patented technology without license
- Patent evasion: Designing products to circumvent patents

### 3.4 Compliance Violations

Domains MUST NOT be used in violation of:

#### 3.4.1 Regulatory Compliance

- Gambling \(unlicensed\): Operating unlicensed gambling or betting
- Pharmaceuticals: Selling prescription drugs or medical devices without proper licensing
- Financial services: Offering investment, insurance, or financial services without proper authorization
- Telemarketing: Unsolicited marketing calls or TCPA violations \(US\)
- COPPA violations: Collecting data from children under 13 without parental consent
- GDPR violations: Processing personal data in violation of GDPR

#### 3.4.2 Payment Card Industry

- Card fraud: Phishing or stealing card information
- Card testing: Testing stolen card numbers
- Carding: Unauthorized use of payment cards

#### 3.4.3 Misleading Practices

- False advertising: Deceptive advertising or marketing claims
- Pyramid schemes: Multi-level marketing schemes
- Lottery scams: Fake lottery or prize schemes
- Miracle cures: Fraudulent health claims or fake medications

---

## 4. DOMANENNAME’S DEFINITION OF ABUSE

### 4.1 What Constitutes Abuse

Domanenname considers the following conduct "abuse":

Technical Abuse:

- Open mail relay or DNS recursion \(allowing third parties to use) Tj ET BT /F1

- DNS amplification attacks or reflection attacks
- Port scanning or network reconnaissance from the domain
- Brute force attacks targeting other services
- Hosting or running botnets, proxies for attacks

Service Abuse:

- Spamming or unsolicited communications
- Multiple complaints from third parties about the domain’s use
- Reselling or redistributing the domain for prohibited purposes
- Using the domain as a proxy to evade other restrictions

Policy Abuse:

- False or misleading registration information
- Knowingly registering for prohibited purposes
- Registering to impersonate another person or entity
- Registering specifically to avoid consequences of previous domain cancellation

### 4.2 Indicators of Abuse

Domanenname monitors for:

- Spam reports: Complaints from ISPs, anti-spam organisations \(Spamhaus, URIBL, etc.\)
- Malware reports: Detection by security firms \(VirusTotal,) Tj ET BT /F1 11 T

- Phishing reports: Reports to anti-phishing organisations
- Traffic analysis: Unusual patterns suggesting abuse
- Content analysis: Automated or manual review of hosted content
- Third-party reports: Complaints from users, trademark holders, copyright owners
- Law enforcement: Reports from law enforcement or security agencies

### 4.3 Reputation Monitoring

Domanenname uses third-party services to monitor domain reputation:

Services Used:

- Spamhaus DNS Blocklist \(DNSBL\)
- SURBL \(Spam URI Real-time Block Lists\)
- VirusTotal \(malware detection\)
- URLhaus \(malware distribution\)
- Phishtank \(phishing site database\)
- Google Safe Browsing \(malware and phishing\)
- Abuse.ch \(malware tracking\)

If Listed:

- Domain owner notified immediately
- Remediation steps provided
- Opportunity to cure before suspension
- Permanent listing may result in cancellation

---

## 5. CONSEQUENCES OF VIOLATIONS

### 5.1 Consequences Escalation

Violations of this policy result in escalating consequences:

**5.1.1 Level 1: Warning \(Minor First Violation\)**

- Trigger: First minor violation; no harm demonstrated
- Action: Email warning sent to account holder
- Response Required: Customer must acknowledge and agree to comply
- Monitoring: Account subject to 30-day monitoring period

Examples:

- Incomplete removal of infringing content after request
- First spam complaint not yet substantiated
- First configuration issue enabling abuse

**5.1.2 Level 2: Conditional Suspension \(Moderate Violation\)**

- Trigger: Second violation or first moderate violation
- Action: Domain suspended; customer contacted immediately
- Requirement: Customer must take corrective action to remedy
- Cure Period: 5-10 working days to remedy and provide evidence
- Timeline: If not cured, proceeds to permanent suspension

Examples:

- Continued spam after warning
- Malware discovered and not removed within 24 hours
- Repeated phishing attempts
- Multiple copyright complaints

**5.1.3 Level 3: Permanent Suspension \(Serious/Repeated Violation\)**

- Trigger: Failure to cure Level 2, or serious violation
- Action: Domain permanently suspended; no cure period
- Access: Customer cannot access or modify domain
- Expiration: Domain remains suspended until expiration
- Recovery: No recovery possible
- Refund: No refund of registration fees

Examples:

- Malware hosting; criminal activity
- Child exploitation material
- After-warning repeated phishing
- Botnet command and control

**5.1.4 Level 4: Cancellation and Account Termination \(Severe/Criminal) Tj ET BT**

- Trigger: Severe criminal activity; imminent harm
- Action: Domain cancelled immediately; account terminated

- Record: Incident documented and reported to authorities if appropriate
- Escalation: May be reported to law enforcement, ICANN, registries
- Consequence: Account banned; customer prohibited from future registrations

Examples:

- Child sexual abuse material
- Ongoing money laundering
- Botnet infrastructure
- Imminent threat to public safety

### 5.2 Immediate Suspension Without Warning

The following violations may result in immediate suspension without warning or cure period:

- Child exploitation material: Automatic immediate suspension
- Malware: Malicious software detected; immediate suspension until remediated
- Botnet: Command and control infrastructure; immediate suspension
- Law enforcement request: Upon legal demand; immediate compliance
- Active fraud: Ongoing theft or financial fraud; immediate suspension
- Imminent harm: Situations where delay would cause serious harm

### 5.3 Domain Deletion and Account Closure

Domanenname reserves the right to:

- Delete the domain from the registry \(permanently\)
- Terminate the customer account \(no future registrations\)
- Block payment methods associated with the account
- Report to authorities \(law enforcement, ICANN, registries\)
- Pursue legal damages for harm caused
- Revoke WHOIS Privacy \(if active\)

---

## 6. INVESTIGATION AND ENFORCEMENT

### 6.1 Domanenname’s Investigation Rights

Upon suspected violation, Domanenname has the right to:

#### 6.1.1 Evidence Gathering

- Review domain configuration and DNS records
- Examine website content and hosted files

- Access server logs and traffic data
- Review email records and communications
- Collect complaints and reports from third parties
- Request information from customer

#### 6.1.2 Cooperation with Authorities

- Respond to law enforcement requests
- Provide data to ICANN, registries, or regulators
- Participate in abuse investigations
- Preserve evidence for legal proceedings
- Cooperate with other registrars and ISPs

#### 6.1.3 Technical Analysis

- Conduct malware scans and vulnerability tests
- Analyse traffic patterns
- Review DNS configurations
- Check for open relays, proxies, or compromises
- Monitor reputation lists and blacklists

### 6.2 Customer Notification

Domanenname will notify customers of:

- Specific abuse allegation or violation
- Evidence supporting the claim \(where legally permissible\)
- Consequences and remediation required \(if applicable\)
- Cure period \(if applicable\)
- Appeal process

Notification Method:

- Email to account holder and administrative contact
- Email to address on file
- Control panel notification \(if applicable\)
- Within 48 hours of determination \(where time-sensitive\)

### 6.3 Investigation Timeline

Abuse Investigation Process:

| Step | Timeline | Action | |------|----------|--------| | Report Received | Immediately | Ticket created; severity assessed | | Initial Review | 24 hours | Preliminary investigation; notification sent | | Detailed Investigation | 2-5 days | Evidence gathered; analysis conducted | | Decision | 5-10 days | Determination of violation; consequences determined | | Notification | Same day as decision | Customer informed of decision and next steps | | Cure Period \(if applicable\) | 5-10 days | Customer has time to remediate | | Enforcement | Upon deadline | Suspension or cancellation implemented |

### 6.4 Emergency Situations

For urgent abuse with immediate harm risk:

- Immediate suspension without investigation delay
- Examples: Active malware, ongoing fraud, child exploitation, botnet
- Customer notified within 24 hours
- Full investigation conducted post-suspension
- Appeal available after investigation complete

---

## 7. CUSTOMER RESPONSIBILITY

### 7.1 Customer Obligations

All customers are responsible for:

#### 7.1.1 Legitimate Use

- Using the domain only for lawful purposes
- Complying with all applicable laws
- Complying with this Acceptable Use Policy
- Complying with ICANN policies
- Complying with local and national laws

#### 7.1.2 Security

- Securing your account with strong passwords
- Enabling two-factor authentication
- Not sharing account credentials
- Protecting against account compromise
- Monitoring account for unauthorized access
- Reporting account compromise immediately

#### 7.1.3 Content Management

- Reviewing content hosted on your domain
- Ensuring content does not violate this policy
- Removing infringing content when requested
- Complying with takedown notices
- Not allowing third parties to host prohibited content

#### 7.1.4 Third-Party Use

- If others use your domain, you are responsible for their use
- Ensure third parties comply with this policy
- Monitor third-party use of your domain

- Implement appropriate controls and agreements
- Remove third-party access if violations occur

#### 7.1.5 Abuse Reporting

- Report abuse of your domain to Domanenname immediately
- If your domain is compromised, notify support at once
- If you receive abuse complaints, respond promptly
- Cooperate with investigations

### 7.2 Liability for Domain Use

Important: As the registered owner, you are liable for:

- All uses of the domain
- Content hosted on the domain \(even if by others\)
- Emails sent from the domain
- All services accessed via the domain
- Third-party use if you allow or enable it

You cannot claim: "I didn’t know" or "Someone else used it" as a defense if you failed to monitor or secure the domain.

### 7.3 Due Diligence

Customers should:

- Review domain content regularly
- Monitor for unauthorized changes
- Check DNS records for unexpected modifications
- Review email security \(SPF, DKIM, DMARC\)
- Stay informed about domain reputation
- Respond to abuse complaints promptly

---

## 8. APPEAL PROCESS

### 8.1 Right to Appeal

If your domain is suspended or cancelled, you have the right to appeal the decision:

Exceptions:

- Child exploitation material \(no appeal\)
- Law enforcement demands \(no appeal\)
- Severe criminal activity \(appeal considered but unlikely to) Tj ET BT /F1 11

### 8.2 Appeal Procedure

Step 1: Request Appeal

- Email: support@domanenname.com
- Subject: "Appeal - Domain Suspension/Cancellation - [Domain Name]"
- Include:
  - Domain name
  - Suspension/cancellation date
  - Your explanation of the situation
  - Evidence contradicting the allegation
  - Remediation steps taken \(if applicable\)

Step 2: Initial Response

- Confirmation received within 24 hours
- Case number assigned
- Appeal acknowledged

Step 3: Appeal Review

- Independent review \(not original investigator, if possible\)
- Detailed consideration of customer’s evidence
- Re-evaluation of original findings
- Investigation timeline: 10-15 working days

Step 4: Appeal Decision

- Written decision provided
- Detailed explanation of reasoning
- If upheld: Next appeal process \(if available\)
- If reversed: Domain unsuspended immediately; service restored

### 8.3 Appeal Grounds

Valid grounds for appeal:

- Factual error: Original investigation reached incorrect conclusion
- New evidence: Evidence not available during original investigation
- Disproportionate response: Punishment exceeded the violation severity
- Procedural error: Incorrect process followed in investigation
- Mistaken identity: Domain confused with another domain
- Technical issue: False positive from automated systems

Not valid grounds:

- Disagreement with policy
- Personal hardship or financial loss
- That you were unaware of the policy

### 8.4 Second Appeal

If appeal is denied, a second appeal is available:

Escalation to Management:

- Email: legal@domanenname.com
- "Second Appeal - [Domain Name] - [Original Case Number]"
- Senior management review
- Response within 15 working days
- Final decision from Domanenname

### 8.5 External Appeals

If second appeal is denied, customers may seek review through:

- ICANN: If ICANN policy violation
- Registrar dispute: Contact with registry
- Legal action: Civil court proceedings
- Alternative Dispute Resolution: Mediation or arbitration

---

## 9. THIRD-PARTY COPYRIGHT AND TRADEMARK NOTICES

### 9.1 DMCA Complaints \(USA\)

For customers with domains subject to USA law, the Digital Millennium Copyright Act \(DMCA\) provides a notice-and-takedown procedure:

Notification Requirements:

- Written notice to domanenname
- Include identification of copyrighted work
- Include location/URL of infringing content
- Include your contact information
- Certification under penalty of perjury that claim is accurate

Domanenname Response:

- Notice sent to domain owner \(customer\)
- Customer has 10 days to respond/dispute
- If not disputed, content removed or domain suspended
- If disputed, matter may proceed to legal system

### 9.2 Trademark Complaints

For trademark infringement claims:

Complaint Process:

- Send notice to legal@domanenname.com

- Include trademark registration details
- Include evidence of infringement
- Include jurisdiction where trademark registered
- Include proposed remedy \(removal, cancellation, transfer\)

Domanenname Response:

- Investigation within 5-10 days
- Notification to domain owner
- If infringement confirmed: Remediation required
- Dispute resolution available for contested claims

### 9.3 Expedited Response

For emergency situations \(active fraud, imminent harm\):

- Email: legal@domanenname.com
- Subject: "Urgent: [Domain Name]"
- Fastest possible response and action

---

## 10. PROHIBITED USES - SPECIFIC EXAMPLES

### 10.1 Phishing Examples \(Prohibited\)

These domain uses are prohibited as phishing:

- Domain "paypa1.com" \(looks like PayPal\) requesting login credentials
- Domain "bank-security-verification.com" sending fake bank emails
- Domain "amazon-account-alert.com" requesting payment information
- Domain "social-verification-service.com" asking for account details

Remedy if Suspected: Report to anti-phishing organization and Domanenname immediately.

### 10.2 Malware Hosting Examples \(Prohibited\)

These domain uses are prohibited as malware hosting:

- Download links to executable files containing viruses
- Automated drive-by download attacks
- Ransomware distribution
- Remote access trojans
- Spyware or info-stealing software

Remedy if Suspected: Report to security firm \(VirusTotal,) Tj ET BT /F1 11 Tf 1

### 10.3 Copyright Piracy Examples \(Prohibited\)

These domain uses are prohibited as copyright infringement:

- Links to pirated movies or TV shows
- Torrent files for copyrighted games
- eBook piracy sites
- Software cracks and keygens
- Unauthorized streaming of copyrighted content

Remedy if You Hold Copyright: Send DMCA notice to Domanenname with evidence.

### 10.4 Cybersquatting Examples \(Prohibited\)

These domain uses are prohibited as cybersquatting/trademark violation:

- "microsft.com" \(Microsoft typosquat\) selling software
- "applle-store.com" \(Apple typosquat\) with fake products
- "bankofengla1nd.com" \(legitimate bank impersonation\)
- "amaz0n-official.com" \(Amazon impersonation with store\)

Remedy if Trademark Holder: File UDRP complaint or send notice to Domanenname.

---

## 11. COMPLIANCE WITH LOCAL LAWS

### 11.1 Multi-Jurisdictional Compliance

Domanenname enforces this policy globally, but compliance with local laws is customer’s responsibility:

Customers must comply with:

- Laws of the country where domain is registered
- Laws of the country where content is hosted
- Laws of countries where domain is accessible
- Laws of the customer’s jurisdiction
- International laws applicable to the activity

### 11.2 Legal Ambiguity

If legality of domain use is unclear:

- Consult legal counsel in your jurisdiction
- Contact local regulatory bodies for guidance
- If in doubt, do not proceed
- Domanenname may suspend pending legal clarity

### 11.3 Jurisdiction-Specific Rules

Examples of jurisdiction-specific rules:

- Gambling: Legal in some jurisdictions, prohibited in others
- Pharmaceuticals: Prescription drug sales permitted in some, prohibited in others
- Financial services: Regulations vary by country
- Content: Some speech protected in some jurisdictions, banned in others

Domanenname Position: Enforcement depends on applicable laws; customer responsible for compliance in their jurisdiction.

---

## 12. MONITORING AND ENFORCEMENT MECHANISMS

### 12.1 Automated Monitoring

Domanenname uses automated systems to detect abuse:

Systems Include:

- Malware scanners: Regular scans of domain content
- Spam filters: Monitoring for spam-related activity
- IP reputation: Monitoring IP reputation lists
- DNSBL monitoring: Checking against spam blacklists
- Traffic analysis: Unusual patterns or behavior
- Content scanning: Automated keyword and pattern matching

### 12.2 Limitations of Automation

Important Note:

- Automated systems not perfect; false positives can occur
- Manual review follows any automated action
- Appeal process available for incorrect automated decisions
- Humans review all suspension/cancellation decisions

### 12.3 Regular Audits

Domanenname conducts:

- Quarterly compliance audits
- Annual policy reviews
- Third-party security assessments
- Reputation list monitoring
- Registrar partner collaboration

---

## 13. ZERO-TOLERANCE ITEMS

### 13.1 Absolutely Prohibited - No Second Chances

The following activities result in immediate permanent suspension with NO appeal or cure period:

- Child sexual abuse material \(CSAM\)
- Active botnet command and control
- Illegal weapons trafficking
- Drug trafficking \(illegal substances\)
- Terrorism-related activity
- Money laundering for criminal organisations
- Ongoing fraud causing financial harm
- Law enforcement blocklist: Domains on law enforcement blocklist \(e.g., FBI, Interpol\)

These are reported to authorities immediately and domain cancelled permanently.

---

## 14. POLICY CHANGES AND UPDATES

### 14.1 Changes to Policy

Domanenname may update this Acceptable Use Policy:

Notice Requirement:

- 30 days’ advance notice via email
- Notice published on website
- Notification in control panel

Customer Rights:

- Customers have 30 days to comply with new policy
- Or cancel domain without penalty
- Continued use = acceptance of new policy

### 14.2 Policy Review

This policy is reviewed:

- Annually: Full comprehensive review
- Quarterly: Updated for known threats and abuse types
- As needed: In response to new legal requirements or significant incidents

---

## 15. CONTACT INFORMATION

For Abuse Reports:

- Email: abuse@domanenname.com
- Web Form: https://domanenname.com/report-abuse
- Urgent line: https://domanenname.com/report-abuse-urgent
- Include: Domain name, type of abuse, evidence/URL

For Appeals:

- Email: support@domanenname.com
- Subject: "Appeal - [Domain Name]"
- Include case number from original suspension

For Questions:

- Email: support@domanenname.com
- Web: https://domanenname.com/support
- Hours: 9 AM - 6 PM CET, Monday to Friday

For Legal Notices:

- Email: legal@domanenname.com
- Address: 7 Bell Yard, London, England, WC2A 2JR

---

## 16. GOVERNING LAW

This Acceptable Use Policy is governed by:

- Laws of England and Wales
- ICANN Policies and Procedures
- Applicable international law
- Local laws of jurisdiction where activity occurs

Jurisdiction:

- Courts of England and Wales have jurisdiction
- ICANN UDRP arbitration may apply for domain disputes

---

Version: 1.0 Last Updated: 18th May 2026 Next Review: 31st December 2026 Effective Date: 18th May 2026

Approved by: CRISALEO LIMITED Legal & Compliance Team

---

Important Disclaimer: This policy must be read in conjunction with Domanenname’s Terms of Service and all applicable policies. In the event of conflict, the most restrictive interpretation will be applied to ensure regulatory compliance and customer protection.