SECURITY WHITE PAPER

OUR COMPREHENSIVE MEASURES TO SAFEGUARD SENSITIVE DATA

IP.com

SECURITY WHITE PAPER

TABLE OF CONTENTS

1 **Overview**

2 **Data Center & Network Security**

Physical Security
- Facilities
- On-site Security
- Monitoring
- Location

Network Security
- Security Team
- Protection
- Network Vulnerability Scanning
- Third-Party Penetration Tests
- Security Incident Event Management (SIEM)
- Anti-Malware
- Logical Access
- Security Incident Response

Encryption
- Encryption in Transit
- Encryption at Rest

5 **Application Security**

Secure Development
- Quality Assurance
- Separate Environments

Application Vulnerabilities
- Dynamic Vulnerability Scanning
- Security Penetration Testing

6 **Product Security Features**

Authentication Security
- Authentication Options
- On-site Security
- Single Sign-on (SSO)
- Secure Credential Storage

Additional Product Security Features
- Access Privileges & Roles
- Transmissions Security
- IP Restrictions
- ITAR Compliance

IQ Ideas+ Security Protocols
- User & Organization Separation
- Sharing Restrictions
- Example Sourcing
- Communication with External Systems
- Application Layer Security Measures

7 **Additional Security Methodologies**

Security Awareness
- Policies
- Training

Employee Security
- Background Checks
- Confidentiality Agreements
- On-Site Office Security

Access Control & Authentication
- Access Restrictions
- Identity Management
- Multi-Factor Authentication (MFA)

SECURITY WHITE PAPER

OVERVIEW

At IP.com, safeguarding customer information, confidentiality, and security is our utmost priority. Since 2001, organizations, universities, and government entities have entrusted us with their most sensitive data. With that trust, we enforce strict security policies and maintain a secure application design to ensure the continued delivery of protected and confidential services that our clients expect.

HIGHLIGHTS

All IP.com computing resources are presently located within the United States, with our InnovationQ+, IQ Ideas+, and other IP.com applications (and supporting facilities) hosted by Amazon Web Services (AWS) and at third-party, secure co-location facilities.

Sensitive data transmission is protected using industry-standard encryption protocols. Your data is encrypted both in transit between you and IP.com servers via HTTPS and Transport Layer Security (TLS1.2 or higher), and at rest using the industry-standard AES-256 algorithm.

User information submitted though our InnovationQ+, IQ Ideas+, Prior Art Database, and IP Analytics Reports are stored in our data centers featuring a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multi-factor authentication mechanisms for access control, and security breach alarms.

Our network is protected by redundant network and web application firewalls, best-in-class router technology, secure HTTPS transport over public networks, regular audits including third-party penetration testing, and Intrusion Detection and/or Prevention technologies (IDS/IPS) that monitor and/or block malicious traffic and network attacks.

Our office facilities, storing client contracts and client confidential emails employ secure keycard entry, breach alarms, and recorded video surveillance. All communication with IP.com personnel is considered confidential information and protected as such.

PHYSICAL SECURITY

Facilities

IP.com's applications are hosted by Amazon Web Services (AWS), and at third-party, secure co-location facilities. AWS's global data center infrastructure is designed to ensure the highest level of performance and availability. AWS and our third-party hosting provider engage with external certifying bodies and independent auditors to provide considerable information regarding policies, processes, and controls resulting in certifications, audit reports, or attestations of compliance such as SOC 2, ISO 27001, ISO 27017 and CSA.

On-Site Security

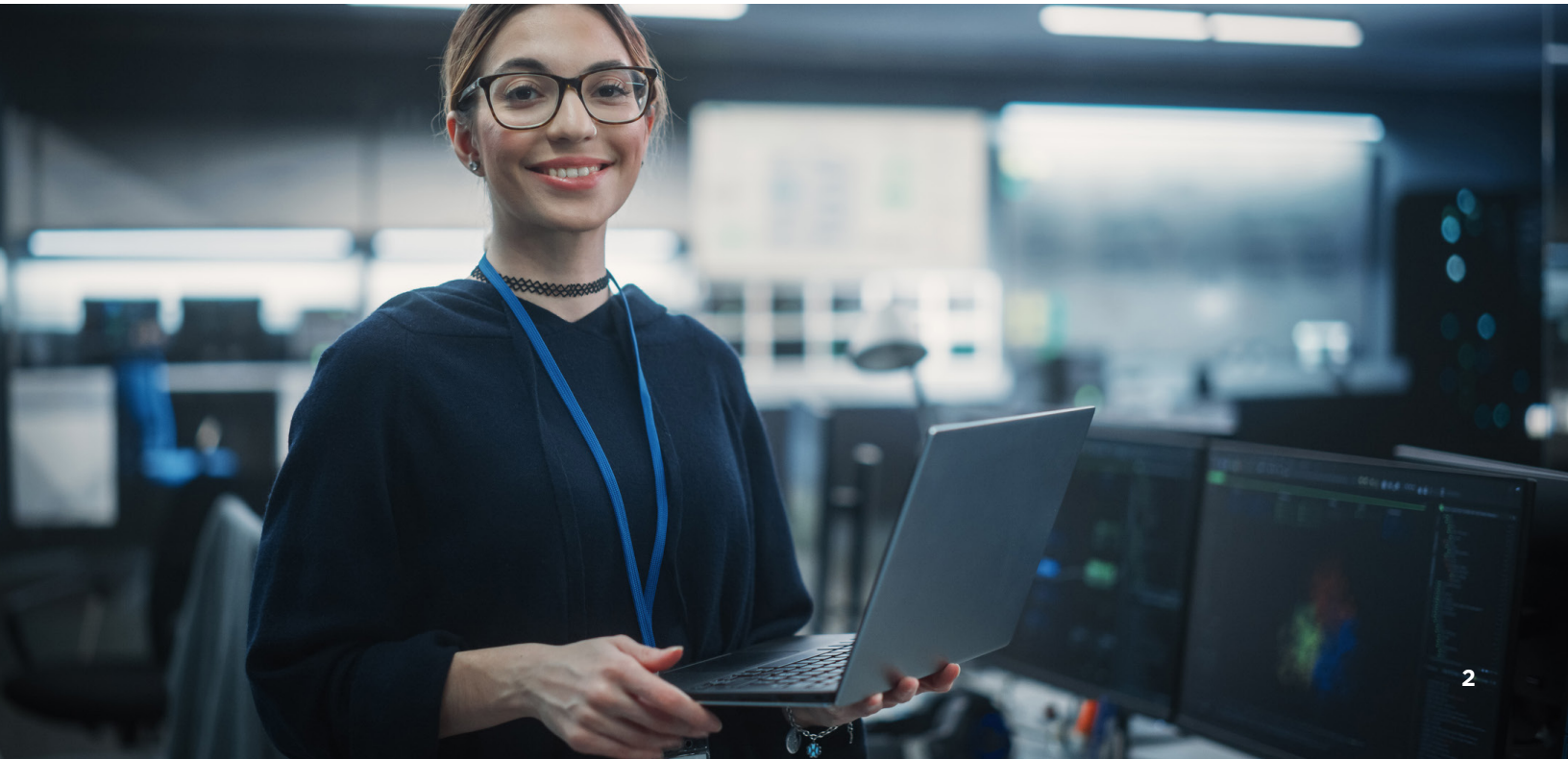
Our data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multi-factor authentication mechanisms for access control and security breach alarms.

Monitoring

All IP.com infrastructure, network systems, and devices are constantly monitored and logically administered by IP.com staff. Physical security, power, and internet connectivity are monitored by the individual facility providers.

Location

All IP.com computing resources are presently located within the United States.



NETWORK SECURITY

Security Team

Our Security Team is on call 24/7 to respond to security alerts and events.

Protection

Our network is protected by redundant network and web application firewalls, best-in-class router technology, secure HTTPS transport over public networks, regular audits, managed endpoint protection and Intrusion Detection and/or Prevention technologies (IDS/IPS) which monitor and/or block malicious traffic and network attacks.

Network Vulnerability Scan

Weekly network security scanning gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems

Third-Party Penetration Tests

In addition to our extensive internal scanning and testing program, each year IP.com employs independent third-party security experts to perform penetration testing across IP.com's Production Network.

Security Incident Event Management (SIEM)

Our Security Incident Event Management (SIEM) program monitors logs from important network devices and host systems and alerts on triggers which notify the Security team for investigation and response.

Anti-Malware

IP.com uses industry leading anti-malware solutions to protect against threats including malware, viruses, Trojans, and spyware. New anti-malware patterns and updates are applied frequently to ensure protection against the latest threats. Best in class endpoint protection with managed detection and response is deployed on all of our systems.

Logical Access

Access to IP.com networks is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored.

Security Incident Response

In case of a system alert, events are escalated to our 24/7 teams providing Operations, Network Engineering, and Security coverage. Employees are trained on security incident response processes, including communication channels and escalation paths.

ENCRYPTION

Encryption in Transit

Communications between you and the IP.com application servers are encrypted via HTTPS and Transport Layer Security (TLS1.2 or higher) over public networks. TLS is also supported for encryption of emails.

Encryption at Rest

All client data submitted through our InnovationQ+, IP Analytics Reports, and IQ Ideas+ services or otherwise mutually deemed to be considered sensitive or confidential is encrypted at rest using the industry-standard AES-256 algorithm.

SECURE DEVELOPMENT

Quality Assurance

Our QA department reviews and tests our code base. Application security engineers on staff identify, test, and triage security vulnerabilities in code.

Separate Environments

Development, Testing, and Staging environments are separated from the Production environment. Client data is not used in non-production environments.

APPLICATION VULNERABILITIES

Dynamic Vulnerability Scanning

We employ third-party, qualified security tools to regularly scan our application against security flaws. Application security engineers test and work with engineering teams to remediate any discovered issues.

Security Penetration Testing

In addition to our extensive internal scanning and testing program, IP.com employs third-party security experts annually to perform detailed application scans and penetration tests on our applications.

AUTHENTICATION SECURITY

Authentication Options

The IP.com applications support login using your IP.com username/password combination. We also support single sign-on (SSO) using industry standard protocols.

On-site Security

Our data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multi-factor authentication mechanisms for access control and security breach alarms.

Single Sign-on (SSO)

Single sign-on (SSO) allows you to authenticate users in your own systems without requiring them to enter additional login credentials for your IP.com application using Security Assertion Markup Language (SAML).

Secure Credential Storage

IP.com follows secure credential storage best practices by never storing passwords in human readable format, and only as the result of a secure, salted, one-way hash.

ADDITIONAL PRODUCT SECURITY FEATURES

Access Privileges & Roles

Access to data within IP.com's applications is governed by access rights and can be configured to define granular access privileges. IP.com has various permission levels for users.

Transmissions Security

All communications with IP.com's servers are encrypted using industry-standard HTTPS over public networks. This ensures that all traffic between you and IP.com is secure during transit. Additionally, our email systems use Transport Layer Security (TLS) to encrypt and deliver email securely, mitigating eavesdropping and spoofing between mail servers.

IP Restrictions

IP.com's applications can be configured to only allow access from specific IP address ranges you define.

ITAR Compliance

IP.com ensures compliance with ITAR regulations. We uphold strict adherence to these regulations by exclusively employing U.S. citizens who have access to our applications and data center facilities. This commitment ensures that sensitive defense-related information and services are handled in accordance with U.S. export control laws and regulations.

IQ IDEAS+ SECURITY PROTOCOLS

User & Organization Separation

The IQ Ideas+ platform securely separates users and organizations by using login information and permissions. Ideas are stored in records tied to creators and their organizations. Only creators and authorized recipients can access these ideas.

Sharing Restrictions

Ideas on the platform are restricted to sharing within the same company, as verified through session and user authentication. Users can only access ideas they've created or have been forwarded by users within their company.

Example Sourcing

Examples are drawn from public Wikipedia data and delivered through our Semantic Gist search engine. Your ideas remain confidential and will never be used beyond your company.

Communication with External Systems

The IQ Ideas+ platform communicates only with internal systems for authentication, generating examples, and emailing users about newly forwarded ideas within their own company. External system engagement is avoided to uphold data security and confidentiality.

Application Layer Security Measures

The platform enforces robust Application Layer security measures. User sessions expire after 3 hours to prevent idle computers from staying logged in. All requests are encrypted using industry-standard protocols to secure data in transit between users and IP.com servers. Both client and server-side validation ensure access to valid user sessions only, denying unauthorized requests. Additionally, user input is sanitized to thwart SQL injection and XSS attacks, bolstering overall platform security.

ADDITIONAL SECURITY METHODOLOGIES

SECURITY AWARENESS

Policies

IP.com has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to, all employees and contractors with access to IP.com information assets.

Training

All employees are subject to our Security Awareness Training which is given continuously throughout the year. Additional security awareness updates are provided via email, blog posts, and in presentations during internal events.

EMPLOYEE SECURITY

Background Checks

IP.com performs background checks on all new employees and contractors in accordance with local laws. The background check includes criminal, education, and employment verification.

Confidentiality Agreements

All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.

On-Site Office Security

Our office facilities employ secure keycard entry, breach alarms and recorded video surveillance.

ACCESS CONTROL & AUTHENTICATION

Access Restrictions

Access to IP.com networks is strictly regulated based on an explicit need-to-know basis, employing the principle of least privilege. This ensures that only individuals with a legitimate requirement can access specific resources, reducing the risk of unauthorized data exposure.

Identity Management

To manage user access effectively, IP.com utilizes Okta, a leading identity and access management platform. Okta centralizes user authentication processes, enabling granular control over access permissions and ensuring that only authorized users can interact with our systems.

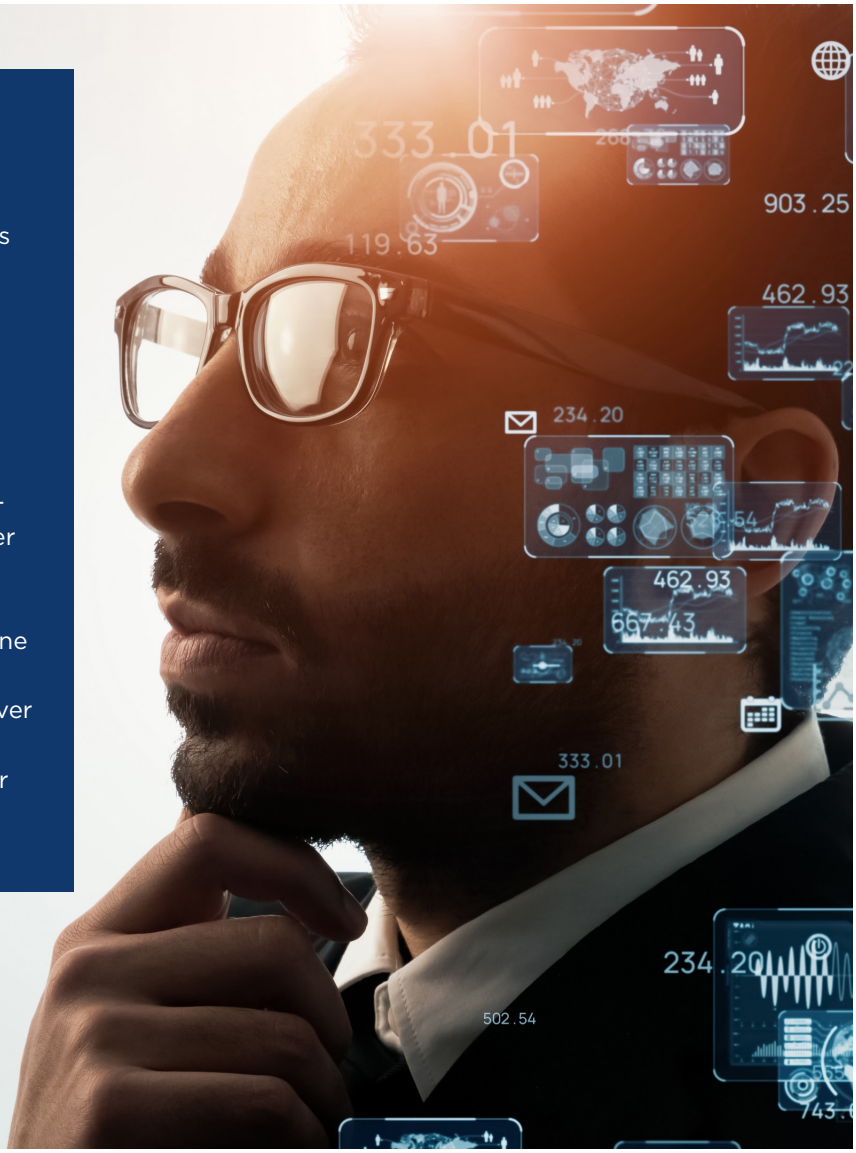
Multi-Factor Authentication (MFA)

As an additional security measure, IP.com enforces Multi-Factor Authentication (MFA) across its platforms. By requiring users to provide two forms of authentication before accessing sensitive resources, we bolster our defense against unauthorized access attempts, enhancing overall security posture.

About IP.com®

Designed for users throughout the innovation lifecycle, our suite of solutions and services deliver insights and results. IP.com's intellectual property software is ideal for IP professionals, research and development teams, inventors and entrepreneurs, and more.

Our solutions are designed to save you money and time using proprietary, state-of-the-art AI. Our goal is to make it easier for organizations to accelerate research and development and enable the rapid evaluation of intellectual property. Fortune 1000 companies, governments, research universities, and top inventors from all over the world use our intelligence solutions to increase efficiencies and improve their innovation processes.



UNLOCK YOUR TRUE INNOVATION POTENTIAL

Connect with our experts:
sales@ip.com

IP.com