SECURITY SOLUTIONS
RISK MANAGED SECURITY ASSURED

Document Classification
Internal Use Only

Acceptable Use Policy

Document Title: Acceptable Use Policy
Document Owner: Founder/CISO
Version: 1.0
Effective Date: Dec 19, 2025
Review Frequency: Annually
Next Review Date: Dec 19, 2026

Version History

Version	Date	Author	Changes
1.0	19/12/2025	Founder/CISO	Initial release of Acceptable use policy

1. Introduction

This Acceptable Use Policy establishes guidelines for the appropriate use of Security Solution Consultants' information technology resources, including the GRCLens platform, computer systems, networks, email, internet access, mobile devices, and related technology assets.

The purpose of this policy is to protect our organization, employees, clients, and partners from security risks, legal liabilities, and reputational harm that may arise from inappropriate use of IT

resources. All users are responsible for using company technology assets in an ethical, lawful, and professional manner.

> **Alignment:** ISO 27001:2022 Clause 5.3 (Roles and Responsibilities), Clause 6.1 (Risk Assessment), Clause 8.1 (Operational Planning and Control) • ISO 27002:2022 Control 5.10 (Acceptable use of information and assets), Control 5.15 (Access control), Control 6.2 (Terms and conditions of employment)

2. Scope

This policy applies to:

- **All Personnel:** Full-time employees, part-time employees, contractors, consultants, temporary staff, interns, and any other individuals with authorized access to Security Solution Consultants' IT resources
- **All IT Resources:** Computer hardware, software, networks, servers, cloud services (including GRCLens platform), email systems, internet access, telecommunications, mobile devices, tablets, IoT devices, and any technology assets owned, leased, or managed by Security Solution Consultants
- **All Locations:** Office premises, remote work locations, client sites, home offices, and any location where company IT resources are accessed
- **Personal Devices:** Personal devices (BYOD - Bring Your Own Device) used to access company data, email, or systems when enrolled in our Mobile Device Management (MDM) program

3. User Responsibilities

3.1 General Responsibilities

All users of Security Solution Consultants' IT resources must:

- Use IT resources primarily for legitimate business purposes related to their role
- Protect confidential and sensitive information in accordance with data classification policies
- Maintain the security and integrity of systems and data entrusted to them
- Report any suspected security incidents, policy violations, or suspicious activity immediately
- Comply with all applicable laws, regulations, and organizational policies
- Respect intellectual property rights, copyrights, trademarks, and licenses

- Use IT resources in a manner that does not disrupt business operations or network performance
- Complete mandatory security awareness training as assigned

3.2 Account and Password Security

- **Unique Credentials:** Never share user accounts, passwords, or authentication credentials with anyone, including colleagues, supervisors, or IT support (IT will never ask for your password)
- **Strong Passwords:** Create strong, unique passwords for all accounts (minimum 12 characters, combination of uppercase, lowercase, numbers, and special characters)
- **Multi-Factor Authentication (MFA):** Enable and use MFA on all systems where available (mandatory for GRCLens platform and email access)
- **Password Management:** Use the approved password manager for storing and generating passwords
- **Immediate Reporting:** Report compromised credentials immediately to the IT security team
- **Session Management:** Log out or lock your workstation when leaving it unattended (automatic timeout after 15 minutes of inactivity)

3.3 Data Protection and Confidentiality

- Handle all company and client data according to its classification level (Public, Internal, Confidential, Restricted)
- Do not store sensitive or confidential data on personal devices unless authorized and encrypted
- Use approved cloud storage services only (GRCLens platform, Microsoft OneDrive for Business) - unauthorized cloud storage services (personal Dropbox, Google Drive, etc.) are prohibited for company data
- Encrypt all confidential data when transmitting via email or storing on removable media
- Do not send sensitive information to personal email accounts
- Properly dispose of confidential information using secure shredding or approved data destruction methods

4. Acceptable Use Guidelines

4.1 Computer and Workstation Use

Acceptable Use:

- Business-related tasks and communications
- Professional development and training activities
- Reasonable personal use during breaks (non-business hours) that does not interfere with work
- Accessing approved software and applications for work purposes
- Installing pre-approved software with IT department authorization

Unacceptable Use:

- Installing unauthorized software, applications, or browser extensions
- Disabling, circumventing, or attempting to bypass security controls (antivirus, firewalls, DLP, etc.)
- Using administrator privileges for unauthorized purposes
- Connecting unauthorized devices to the corporate network
- Attempting to access, modify, or delete files or systems without proper authorization
- Running security scanning tools or penetration testing without explicit CISO approval

4.2 Email and Communication Systems

Acceptable Use:

- Business communications with clients, partners, and colleagues
- Professional and respectful communication tone
- Using email signatures with appropriate company branding
- Encrypting emails containing confidential or sensitive information
- Reporting suspicious emails or phishing attempts to IT security
- Limited personal email use that does not interfere with business operations

Unacceptable Use:

- Sending spam, chain letters, or unsolicited mass emails
- Creating, forwarding, or storing offensive, harassing, discriminatory, or inappropriate content
- Impersonating another person or misrepresenting identity
- Using company email for personal business ventures or commercial purposes

- Forwarding company emails to personal email accounts without authorization
- Clicking on links or opening attachments from unknown or suspicious sources
- Auto-forwarding company email to external addresses

4.3 Internet and Web Access

Acceptable Use:

- Business research and information gathering
- Professional networking (LinkedIn for business purposes)
- Online training and professional development
- Accessing cloud-based business applications (GRCLens, Microsoft 365, approved SaaS tools)
- Reasonable personal browsing during breaks that does not consume excessive bandwidth

Unacceptable Use (Prohibited Sites/Activities):

- Accessing, downloading, or distributing pornographic, sexually explicit, or adult content
- Visiting sites containing illegal content, hate speech, or promoting violence
- Online gambling, gaming (non-business), or entertainment streaming during work hours
- Downloading or streaming pirated software, music, movies, or other copyrighted material
- Accessing peer-to-peer (P2P) file sharing networks or torrent sites
- Using anonymizing proxies, VPNs, or tools to bypass web filtering (unless approved for work)
- Excessive personal shopping, social media use, or non-work browsing during business hours
- Cryptocurrency mining or participating in blockchain networks using company resources

4.4 Mobile Devices and Remote Access

Acceptable Use:

- Using company-issued mobile devices for business purposes
- Enrolling personal devices in MDM when accessing company data (BYOD program)
- Using approved VPN for secure remote access
- Keeping mobile devices updated with latest security patches

- Enabling device encryption and screen lock (PIN/biometric)
- Reporting lost or stolen devices immediately

Unacceptable Use:

- Jailbreaking or rooting company-issued devices
- Installing unauthorized applications on company devices
- Disabling or removing MDM profiles without IT authorization
- Accessing company data from public or shared devices
- Using unsecured public Wi-Fi without VPN for accessing company resources
- Sharing mobile devices with unauthorized individuals

5. Strictly Prohibited Activities

The following activities are strictly prohibited and may result in immediate disciplinary action, up to and including termination of employment:

5.1 Illegal Activities

- Engaging in any illegal activity using company IT resources
- Unauthorized access to computer systems (hacking)
- Creating, distributing, or possessing malware, viruses, or malicious code
- Theft of data, intellectual property, or confidential information
- Identity theft, fraud, or impersonation
- Copyright or trademark infringement
- Insider trading or misuse of confidential business information

5.2 Security Violations

- Deliberately introducing viruses, malware, ransomware, or security threats
- Attempting to gain unauthorized access to systems, networks, or data
- Sharing credentials or providing unauthorized access to company systems
- Disabling or circumventing security controls without authorization
- Social engineering attacks against employees or clients
- Exfiltrating company or client data to unauthorized locations

5.3 Harassment and Discrimination

- Creating, viewing, storing, or distributing offensive, harassing, or discriminatory content
- Cyberbullying, harassment, or intimidation of colleagues, clients, or partners
- Using IT resources to make threats or engage in hostile behavior
- Accessing, storing, or distributing pornographic or sexually explicit material

5.4 Business Misuse

- Using company IT resources for personal business ventures or competing businesses
- Conducting unauthorized commercial activities or solicitations
- Excessive personal use that interferes with work responsibilities or network performance
- Misrepresenting the company or making unauthorized public statements on behalf of the organization

5.5 Data and Privacy Violations

- Unauthorized disclosure of confidential company or client information
- Violating data privacy regulations (Australian Privacy Act, GDPR, etc.)
- Accessing client data without legitimate business need or authorization
- Storing sensitive data in unauthorized locations or personal accounts
- Failing to properly dispose of confidential information

6. Software and Licensing

6.1 Software Installation

- Only install software that has been approved by the IT department and is licensed appropriately
- Request software installation through the IT service desk ticketing system
- Do not install trial, freeware, or shareware software without IT approval
- Prohibited: Installing unlicensed, pirated, or cracked software

6.2 License Compliance

- All software must be properly licensed and used in accordance with license agreements

- Do not exceed license entitlements or install software on unauthorized devices
- Company-licensed software may not be used for personal projects or installed on personal devices (unless explicitly permitted by license terms)
- Report any instances of unlicensed software to the IT department

6.3 Cloud Services and SaaS Applications

- **Approved Cloud Services:** GRCLens platform, Microsoft 365, approved business tools only
- **Shadow IT Prohibited:** Do not sign up for or use unauthorized cloud services for business purposes without IT and CISO approval
- All cloud services must undergo security assessment before use
- Do not upload company or client data to personal cloud storage accounts (Dropbox, Google Drive personal, iCloud, etc.)

7. Social Media and Public Communications

7.1 Professional Social Media Use

- Limited personal social media access during work hours is acceptable during breaks
- When posting about work or the company, clearly state you are expressing personal views (not company positions)
- Do not disclose confidential company information, client names, or project details on social media
- Maintain professional conduct - negative posts about the company, colleagues, or clients are prohibited
- Business use of LinkedIn for networking and recruitment is encouraged

7.2 Official Company Communications

- Only authorized personnel (Marketing, CEO, CISO) may make official statements on behalf of Security Solution Consultants
- Do not respond to media inquiries - direct all media contact to the CEO or designated spokesperson
- Do not post confidential information about clients, the GRCLens platform, security controls, or business operations
- Refer to the Social Media Policy for detailed guidelines

8. Monitoring and Privacy

Important Notice: Users should have no expectation of privacy when using Security Solution Consultants' IT resources. By using company technology assets, you consent to monitoring and auditing as described below.

8.1 Monitoring Activities

Security Solution Consultants reserves the right to monitor, audit, access, review, and disclose information obtained through the use of company IT resources, including but not limited to:

- **Network Traffic:** All network traffic, including websites visited, bandwidth usage, and data transfers
- **Email Communications:** All emails sent and received through company email systems (subject lines, content, attachments)
- **System Logs:** Authentication logs, file access logs, application usage, and system activity
- **Endpoint Activity:** Software installed, files accessed, USB device usage, and user behavior
- **GRCLens Platform:** User activity within the GRCLens platform (access, changes, exports)
- **Mobile Devices:** Location data, application usage, and data access on MDM-enrolled devices

8.2 Purpose of Monitoring

Monitoring is conducted for legitimate business purposes including:

- Protecting against security threats, malware, and cyberattacks
- Detecting and preventing data breaches or unauthorized data access
- Ensuring compliance with laws, regulations, and company policies
- Investigating suspected policy violations or misconduct
- Maintaining network performance and system integrity
- Meeting legal or regulatory obligations (audits, e-discovery, investigations)

8.3 Privacy Considerations

- Monitoring is conducted in compliance with Australian privacy laws and workplace monitoring legislation
- Access to monitoring data is restricted to authorized IT security personnel, management, and legal counsel on a need-to-know basis
- Monitoring data is retained in accordance with our Evidence Retention Policy

- Users will be notified in writing prior to any targeted monitoring (where legally required)

9. Incident Reporting

9.1 Reporting Requirements

All users must immediately report the following to the IT Security team:

- Suspected security incidents or data breaches
- Phishing emails or social engineering attempts
- Malware infections or suspicious system behavior
- Lost or stolen devices containing company data
- Compromised credentials or unauthorized access
- Suspected policy violations by colleagues
- Any unusual network activity or system performance issues

9.2 Reporting Channels

Security Support Team:
Email: support@secsolutionshub.com

Phone: [Security Hotline - 24/7]

For Urgent Security Incidents:
Contact CISO directly: [CISO Contact Information]

Anonymous Reporting:
Use the confidential reporting portal: [Whistleblower Portal URL]

9.3 Non-Retaliation

Security Solution Consultants prohibits retaliation against any employee who reports security concerns or policy violations in good faith. Reports can be made anonymously through the whistleblower portal.

10. Enforcement and Consequences

10.1 Policy Violations

Violations of this Acceptable Use Policy may result in disciplinary action, up to and including termination of employment or contractual relationship. The severity of disciplinary action will depend on:

- Nature and severity of the violation
- Whether the violation was intentional or accidental
- Impact on the organization, clients, or colleagues
- History of previous violations
- Level of cooperation during investigation

10.2 Disciplinary Actions

Violation Type	Potential Consequences
Minor Violation (First Offense)	Verbal warning, mandatory retraining, access restrictions
Moderate Violation	Written warning, temporary suspension of IT privileges, performance improvement plan
Serious Violation	Suspension without pay, final written warning, revocation of remote access
Severe/Criminal Violation	Immediate termination, referral to law enforcement, legal action

10.3 Legal Consequences

Serious violations may result in:

- Civil liability for damages caused by policy violations
- Criminal prosecution under Australian cybercrime laws
- Loss of professional certifications or licenses
- Reporting to relevant authorities (OAIC, ACSC, law enforcement)

10.4 Immediate Actions for Serious Violations

- Immediate suspension of all IT access and credentials
- Forensic investigation of user activity
- Collection and preservation of evidence
- Notification to affected parties (if data breach or privacy violation)
- Cooperation with law enforcement investigations

11. User Acknowledgment

By signing below or electronically accepting this policy, I acknowledge that:

- I have read, understood, and agree to comply with this Acceptable Use Policy
- I understand that company IT resources are provided for business purposes and are subject to monitoring
- I have no expectation of privacy when using company IT resources
- I understand that violations of this policy may result in disciplinary action up to and including termination
- I will report any suspected security incidents or policy violations immediately
- I understand this policy may be updated periodically and it is my responsibility to stay informed of changes

Employee/Contractor Name:

Employee ID:

Signature:

Date:

12. Related Policies and References

Related Internal Policies

- Information Security Policy
- Access Control Policy
- Data Classification and Handling Policy
- Encryption Policy
- Mobile Device Management Policy
- Remote Access Policy
- Social Media Policy
- Security Incident Response Plan
- Data Retention and Disposal Policy
- Code of Conduct

External References and Standards

- ISO 27001:2022 - Information Security Management Systems
- ISO 27002:2022 - Information Security Controls
- Australian Privacy Act 1988
- Notifiable Data Breaches (NDB) scheme
- Australian Cyber Security Centre (ACSC) Guidelines
- Fair Work Act 2009 (workplace monitoring provisions)