SECURITY SOLUTIONS
RISK MANAGED SECURITY ASSURED

Code of Conduct Policy

Document Title: Code of Conduct Policy
Document Owner: Chief Information Security Officer
Version: 1.0
Effective Date: Sep 19, 2025
Review Frequency: Annually
Next Review Date: Sep 19, 2026

Version History

Version	Date	Author	Changes
1.0	19/09/2025	CISO	Initial release

Message from Leadership

At Security Solution Consultants PTY LTD, we are committed to maintaining the highest standards of professional conduct, ethical behavior, and integrity in everything we do. As a GRC consulting practice and technology provider, our reputation is built on the trust our clients, partners, and stakeholders place in us.

This Code of Conduct outlines the principles and standards that guide our decisions and actions. It applies to every member of our organization—from executives to employees, contractors, and

consultants. We expect everyone associated with Security Solution Consultants to uphold these standards and to conduct themselves with honesty, respect, and professionalism.

Our success depends not only on delivering exceptional services but also on how we conduct our business. By adhering to this Code of Conduct, we protect our organization, our people, and our clients, while fostering a culture of excellence, accountability, and ethical leadership.

1. Introduction

1.1 Purpose

The purpose of this Code of Conduct Policy is to:

- Establish clear standards of professional and ethical conduct for all personnel
- Define expected behaviors and decision-making principles
- Promote a culture of integrity, respect, accountability, and excellence
- Protect the reputation and interests of Security Solution Consultants PTY LTD
- Ensure compliance with legal and regulatory requirements
- Provide guidance for addressing ethical dilemmas and conflicts
- Foster a safe, inclusive, and respectful workplace environment

1.2 Scope

This Code of Conduct applies to:

- All employees (full-time, part-time, casual) of Security Solution Consultants PTY LTD
- Executives, directors, and officers
- Contractors, consultants, and temporary workers
- Interns and volunteers
- Third-party representatives acting on behalf of Security Solution Consultants

This Code applies to all work-related activities, including:

- During working hours and in the workplace
- At client sites and during client engagements
- At company-sponsored events, conferences, and training sessions
- During business travel
- When representing Security Solution Consultants in any capacity

- In online communications and social media when identifiable as a Security Solution Consultants employee

2. Core Values and Principles

Security Solution Consultants PTY LTD is guided by the following core values that underpin all our activities:

2.1 Integrity

We conduct our business with honesty, transparency, and accountability. We do what we say we will do, and we honor our commitments to clients, colleagues, and stakeholders. We take responsibility for our actions and admit mistakes when they occur.

We demonstrate integrity by: Being truthful in all communications, honoring commitments, admitting errors, avoiding deceptive practices, maintaining accurate records

2.2 Excellence

We are committed to delivering exceptional quality in our services, products, and client relationships. We continuously improve our capabilities, embrace innovation, and strive for excellence in everything we do.

We demonstrate excellence by: Delivering high-quality work, continuously learning and improving, meeting deadlines, exceeding client expectations, embracing best practices

2.3 Respect

We treat everyone with dignity, courtesy, and respect. We value diversity and inclusion, and we foster a workplace environment where all individuals feel valued, heard, and respected regardless of their background, role, or perspective.

We demonstrate respect by: Listening actively, valuing diverse perspectives, treating others with courtesy, using inclusive language, respecting boundaries and privacy

2.4 Accountability

We take ownership of our work, decisions, and actions. We hold ourselves and each other accountable to our values, commitments, and professional standards. We learn from our mistakes and take corrective action when needed.

We demonstrate accountability by: Meeting commitments, taking ownership of outcomes, acknowledging mistakes, following through on responsibilities, supporting team goals

2.5 Confidentiality and Trust

We protect confidential information belonging to our clients, our organization, and our colleagues. We build and maintain trust through discretion, professionalism, and secure handling of sensitive information.

We demonstrate confidentiality by: Safeguarding sensitive information, respecting privacy, complying with data protection requirements, maintaining client confidence, using information appropriately

3. Professional Conduct Standards

3.1 Professional Competence

- **Maintain Competence:** Continuously develop and maintain professional knowledge, skills, and competencies relevant to your role
- **Work Within Competence:** Only perform work for which you have the necessary qualifications, training, and competence, or work under appropriate supervision
- **Seek Guidance:** Ask for help or clarification when uncertain about tasks, requirements, or expectations
- **Professional Development:** Participate in training, professional development, and continuous learning opportunities
- **Quality of Work:** Deliver work that meets professional standards and quality expectations

3.2 Professional Appearance and Demeanor

- **Professional Presentation:** Maintain a professional appearance appropriate to the work environment and client expectations
- **Business Attire:** Dress in business or business casual attire when representing Security Solution Consultants, particularly at client sites and professional events
- **Conduct:** Behave professionally, courteously, and respectfully in all interactions
- **Communication:** Communicate clearly, professionally, and respectfully in all forms (verbal, written, digital)

3.3 Attendance and Punctuality

- Arrive at work, meetings, and client appointments on time
- Notify your manager and relevant parties promptly if unable to attend or if delayed
- Manage time effectively and meet deadlines
- Follow organizational policies regarding leave, flexible work, and remote work arrangements

3.4 Use of Company Resources

- **Appropriate Use:** Use company resources (equipment, systems, time, facilities) only for authorized business purposes
- **Care and Protection:** Protect company assets from damage, loss, theft, or misuse
- **IT Resources:** Follow the Acceptable Use Policy for IT resources and systems
- **Personal Use:** Limited personal use of company resources (email, internet) is permitted if it does not interfere with work responsibilities, consume significant resources, or violate company policies
- **Reporting:** Report damaged, lost, or stolen company property immediately

3.5 Substance Use and Workplace Safety

- **Alcohol and Drugs:** Do not report to work, or work, while under the influence of alcohol or illegal drugs
- **Prescription Medications:** Notify your manager if prescription medications may affect your ability to perform work safely
- **Workplace Safety:** Follow all health and safety policies and procedures
- **Report Hazards:** Report unsafe conditions, accidents, and near-misses immediately
- **Company Events:** Consume alcohol responsibly at company-sponsored events where alcohol is served

4. Ethical Conduct and Integrity

4.1 Honesty and Truthfulness

- **Truthful Communication:** Be honest and accurate in all communications, reports, documents, and representations
- **No Misrepresentation:** Do not make false or misleading statements about qualifications, experience, capabilities, or deliverables
- **Accurate Records:** Ensure all business records, timesheets, expense reports, and documentation are accurate and complete
- **Admit Mistakes:** Acknowledge errors and work to correct them promptly

4.2 Conflicts of Interest

A conflict of interest occurs when personal interests, relationships, or activities interfere (or appear to interfere) with your ability to make objective decisions in the best interests of Security Solution Consultants.

Examples of potential conflicts of interest include:

- Outside employment or business activities that compete with or compromise work for Security Solution Consultants
- Financial interests in clients, suppliers, or competitors
- Close personal or family relationships with clients, suppliers, or competitors
- Accepting gifts, entertainment, or favors from clients or vendors that could influence business decisions
- Using company information, resources, or position for personal gain
- Serving on boards or in advisory roles for organizations that may compete with or conflict with our business

> **Disclosure Requirement:**
>
> All actual or potential conflicts of interest must be disclosed in writing to your manager and the CISO. Most conflicts can be managed through disclosure and appropriate safeguards. Failure to disclose conflicts of interest is a serious breach of this Code of Conduct.

4.3 Gifts, Entertainment, and Hospitality

- **Modest Gifts:** You may accept modest, occasional gifts (value < AU$100) such as promotional items, small tokens of appreciation, or customary business courtesies
- **Business Meals:** Reasonable business meals and entertainment are acceptable if they serve a legitimate business purpose
- **Prohibited Gifts:** Do not accept cash, cash equivalents (gift cards, vouchers), or gifts that could reasonably be perceived to influence business decisions
- **Reporting:** Gifts or entertainment valued at more than AU$100 must be reported to your manager
- **Government Officials:** Special restrictions apply to gifts and hospitality involving government officials— consult with management before offering or accepting

4.4 Bribery and Corruption

- **Zero Tolerance:** Security Solution Consultants has a zero-tolerance policy for bribery, corruption, and improper payments
- **No Bribes:** Do not offer, promise, give, request, or accept bribes, kickbacks, or any form of improper payment to obtain or retain business advantage
- **Facilitation Payments:** Do not make facilitation payments (small payments to expedite routine government actions)
- **Compliance:** Comply with all applicable anti-bribery and anti-corruption laws, including Australian Criminal Code and foreign anti-corruption laws

- **Report Concerns:** Report any suspected bribery or corruption immediately to your manager, CISO, or CEO

4.5 Fair Dealing and Competition

- Compete fairly and ethically in the marketplace
- Do not engage in deceptive, misleading, or unfair business practices
- Respect intellectual property rights of others
- Do not disparage competitors unfairly or make false statements about competitors
- Comply with competition and consumer protection laws
- Do not enter into anti-competitive agreements or arrangements

5. Workplace Conduct and Respectful Behavior

5.1 Discrimination and Harassment

Security Solution Consultants is committed to providing a workplace free from discrimination, harassment, and bullying.

- **Zero Tolerance:** We have zero tolerance for discrimination, harassment, bullying, or victimization of any kind
- **Protected Attributes:** Do not discriminate against or harass anyone based on age, disability, race, color, national origin, religion, sex, gender identity, sexual orientation, pregnancy, family responsibilities, or any other characteristic protected by law
- **Sexual Harassment:** Sexual harassment of any form is strictly prohibited, including unwelcome sexual advances, requests for sexual favors, offensive comments, or conduct of a sexual nature
- **Bullying:** Bullying, intimidation, or abusive behavior is not tolerated
- **Reporting:** Report discrimination, harassment, or bullying immediately to your manager, HR, or via the confidential reporting mechanism
- **No Retaliation:** Retaliation against anyone who reports concerns in good faith is strictly prohibited

5.2 Diversity, Equity, and Inclusion

- Value and respect diversity in all forms
- Treat all individuals with dignity and respect regardless of differences
- Foster an inclusive environment where everyone can contribute and succeed

- Challenge biases and promote equitable treatment and opportunities
- Use inclusive language and avoid stereotypes

5.3 Workplace Violence and Threats

- **Violence-Free Workplace:** Security Solution Consultants is committed to maintaining a safe, violence-free workplace
- **Prohibited Conduct:** Threats, intimidation, physical violence, or aggressive behavior are strictly prohibited
- **Weapons:** Weapons of any kind are prohibited in the workplace and at work-related events (unless authorized by law enforcement personnel)
- **Reporting:** Report any threats, violent behavior, or safety concerns immediately to management or authorities

5.4 Respectful Communication

- Communicate respectfully, professionally, and constructively
- Listen actively and consider diverse perspectives
- Provide and receive feedback constructively
- Avoid gossip, rumors, or disparaging comments about colleagues, clients, or the organization
- Resolve conflicts professionally and respectfully, seeking mediation or management assistance if needed

6. Confidentiality and Information Security

6.1 Confidential Information

- **Protect Confidential Information:** Safeguard confidential information belonging to Security Solution Consultants, clients, partners, and employees
- **Need-to-Know Basis:** Only access, use, or share confidential information when necessary for legitimate business purposes
- **Client Confidentiality:** Protect client information with the highest level of care and discretion
- **Non-Disclosure:** Do not disclose confidential information to unauthorized parties, including family, friends, or external parties
- **Post-Employment:** Confidentiality obligations continue after employment ends

6.2 Information Security Compliance

- **Follow Security Policies:** Comply with all information security policies, procedures, and standards
- **Data Classification:** Handle information according to its classification level (PUBLIC, INTERNAL, CONFIDENTIAL, RESTRICTED)
- **Password Security:** Use strong passwords, do not share credentials, enable multi-factor authentication
- **Secure Devices:** Protect laptops, mobile devices, and storage media from loss, theft, or unauthorized access
- **Phishing Awareness:** Be vigilant about phishing attempts and report suspicious emails
- **Incident Reporting:** Report security incidents, data breaches, or suspected compromises immediately

6.3 Intellectual Property

- **Company IP:** All work product, inventions, and intellectual property created in the course of employment belong to Security Solution Consultants
- **Respect Third-Party IP:** Respect the intellectual property rights of clients, partners, and third parties
- **Proper Licensing:** Ensure all software and materials are properly licensed
- **No Unauthorized Use:** Do not use, copy, or distribute proprietary information or software without authorization

6.4 Privacy and Personal Information

- Comply with Privacy Act 1988 and Australian Privacy Principles (APPs)
- Protect personal information of employees, clients, and other individuals
- Collect, use, and disclose personal information only for lawful and legitimate purposes
- Respect individual privacy rights and data subject rights
- Report privacy breaches or suspected data breaches immediately

7. Client Relations and Service Excellence

7.1 Client Service Standards

- **Client-Centric Approach:** Prioritize client needs and deliver exceptional service

- **Professional Relationships:** Build and maintain professional, respectful relationships with clients
- **Responsiveness:** Respond to client inquiries and requests in a timely and professional manner
- **Quality Deliverables:** Deliver high-quality work that meets or exceeds client expectations
- **Transparency:** Communicate honestly and transparently about project status, challenges, and timelines
- **Scope Management:** Manage project scope professionally and document changes appropriately

7.2 Independence and Objectivity

- **Professional Judgment:** Maintain professional independence and objectivity in all client engagements
- **Unbiased Advice:** Provide objective, unbiased recommendations based on professional expertise and client best interests
- **Avoid Conflicts:** Disclose any relationships or circumstances that could compromise objectivity
- **No Self-Dealing:** Do not use client engagements for personal gain or to benefit competing interests

7.3 Client Confidentiality

- Protect client confidential information with the highest level of care
- Do not discuss client matters in public places or with unauthorized persons
- Do not use client information for personal benefit or competitive advantage
- Comply with client confidentiality agreements and NDAs
- Obtain client permission before using client name, logo, or case studies in marketing materials

7.4 Professional Boundaries

- Maintain appropriate professional boundaries with clients
- Avoid situations that could compromise professional objectivity or create conflicts of interest
- Do not accept personal benefits or favors from clients that could influence professional judgment
- Disclose personal relationships with client personnel that could affect objectivity

8. Compliance with Laws and Regulations

8.1 Legal Compliance

- **Comply with Laws:** Comply with all applicable laws, regulations, and industry standards in Australia and other jurisdictions where we operate
- **Key Laws:** Including but not limited to:
    - Work Health and Safety Act 2011
    - Fair Work Act 2009
    - Privacy Act 1988
    - Competition and Consumer Act 2010
    - Corporations Act 2001
    - Australian Criminal Code (bribery, corruption, fraud)
    - Spam Act 2003
    - Copyright Act 1968
- **Seek Guidance:** If uncertain about legal requirements, consult with management or legal counsel

8.2 Regulatory Compliance

- Comply with ISO 27001:2022 requirements and ISMS policies
- Follow industry-specific regulations applicable to our services (PCI DSS, Essential Eight, etc.)
- Cooperate with regulatory audits and inspections
- Maintain accurate records for compliance purposes

8.3 Export Controls and Trade Sanctions

- Comply with export control laws and trade sanctions
- Do not engage with sanctioned countries, entities, or individuals
- Obtain necessary approvals before transferring controlled technology or information

9. Reporting Violations and Concerns

9.1 Duty to Report

All personnel have a duty to report:

- Violations of this Code of Conduct

- Violations of laws, regulations, or company policies
- Unethical behavior or misconduct
- Security incidents, data breaches, or privacy violations
- Fraud, bribery, or corruption
- Discrimination, harassment, or bullying
- Conflicts of interest
- Safety hazards or workplace violence

9.2 Reporting Channels

You can report concerns through multiple channels:

- **Direct Manager:** Speak with your immediate manager or supervisor
- **Senior Management:** Contact the CISO, CEO, or other senior executives
- **Human Resources:** Contact HR for workplace conduct issues
- **Confidential Hotline:** Use the confidential ethics hotline (email: support@secsolutionshub.com)
- **Anonymous Reporting:** Anonymous reports are accepted (though follow-up may be limited)

9.3 Good Faith Reporting

- Reports should be made in good faith with reasonable belief that a violation has occurred
- Knowingly making false or malicious reports is a violation of this Code
- You are not required to be certain that a violation has occurred, report concerns if you have reasonable suspicion

9.4 No Retaliation Policy

Zero Tolerance for Retaliation:

Security Solution Consultants strictly prohibits retaliation against anyone who reports concerns in good faith or participates in an investigation. Retaliation includes adverse employment actions (termination, demotion, harassment, intimidation) taken because someone reported a concern. Anyone who retaliates will face disciplinary action up to and including termination.

9.5 Investigation Process

- All reports will be taken seriously and investigated promptly and thoroughly
- Investigations will be conducted confidentially to the extent possible
- Personnel are required to cooperate fully with investigations

- Appropriate action will be taken based on investigation findings
- Reporters will be informed of outcomes to the extent permitted by confidentiality and privacy considerations

10. Consequences of Non-Compliance

10.1 Disciplinary Action

Violations of this Code of Conduct will result in disciplinary action appropriate to the nature and severity of the violation, which may include:

- Verbal or written warning
- Mandatory training or counseling
- Performance improvement plan
- Loss of privileges or responsibilities
- Suspension (with or without pay)
- Demotion
- Termination of employment or contract

10.2 Legal Consequences

Certain violations may result in civil or criminal liability, including:

- Civil lawsuits for damages
- Criminal prosecution for illegal conduct (fraud, bribery, theft, assault, etc.)
- Fines, penalties, or imprisonment
- Professional license suspension or revocation
- Regulatory sanctions

10.3 Organizational Consequences

Code violations can also harm Security Solution Consultants through:

- Reputational damage and loss of client trust
- Loss of business opportunities
- Regulatory sanctions and fines
- Legal liability and litigation costs
- Loss of certifications or accreditations

11. Acknowledgment and Certification

All personnel are required to:

- Read and understand this Code of Conduct Policy
- Acknowledge receipt and understanding of the Code
- Certify compliance with the Code annually
- Complete Code of Conduct training as required
- Ask questions if any provisions are unclear

Employee Certification Statement

I certify that I have read, understood, and agree to comply with the Security Solution Consultants PTY LTD Code of Conduct Policy. I understand that violations of this Code may result in disciplinary action up to and including termination of employment. I understand my obligation to report violations and that I will not face retaliation for good faith reporting.

Employee Name (Print):

Employee Signature:

Date:

12. Questions and Guidance

If you have questions about this Code of Conduct or need guidance on ethical dilemmas, contact:

- Your direct manager or supervisor
- Human Resources
- CISO or CEO
- Ethics hotline: support@secsolutionshub.com

Decision-Making Framework:

When faced with an ethical dilemma, ask yourself:

- Is it legal?
- Is it consistent with our values and this Code of Conduct?

- Would I be comfortable if my decision were made public?
- Is it fair to all stakeholders?
- Would I want my family to know about this decision?
- Am I setting a good example for others?

If the answer to any of these questions is "no" or "I'm not sure," seek guidance before proceeding.

13. Related Policies and References

Related Internal Policies

- Information Security Policy
- Acceptable Use Policy
- Data Classification Policy
- Privacy Policy
- Security Awareness Training Policy
- Workplace Health and Safety Policy

External References

- ISO 27001:2022 - Information Security Management Systems
- ISO 27002:2022 - Information Security Controls
- Work Health and Safety Act 2011 (Australia)
- Fair Work Act 2009 (Australia)
- Privacy Act 1988 (Australia)
- Competition and Consumer Act 2010 (Australia)
- Australian Criminal Code (Bribery and Corruption)