SECURITY SOLUTIONS
RISK MANAGED SECURITY ASSURED

DISCIPLINARY PROCESS

Security Solution Consultants PTY. LTD

DOCUMENT CONTROL

Version: 1.0

Effective Date: February 22, 2026

Review Frequency: Annual

Policy Owner: Chief Information Security Officer (CISO)

Approved By: CISO/Founder/Principal Consultant

Next Review Date: February 22, 2027

1. PURPOSE

This Disciplinary Process establishes a fair, consistent, and legally compliant framework for addressing information security breaches and policy violations within Security Solution Consultants PTY. LTD ('the Organization').

This process ensures:

- Fair treatment of all individuals subject to disciplinary action
- Consistent handling of security violations across the organization
- Compliance with applicable employment law in Australia and New Zealand
- Protection of organizational information assets and business interests

2. SCOPE

This disciplinary process applies to all individuals who have access to the Organization's information systems, data, or facilities, including:

- Employees (full-time, part-time, and casual)
- Contractors and subcontractors
- Consultants and professional advisors
- Temporary staff and interns
- Third-party personnel working on behalf of the Organization

Note: The Organization currently has no employees, this policy will become effective upon the onboarding of staff or contractors.

3. APPLICABLE LEGISLATION AND STANDARDS

This policy is designed to comply with the following legislation and standards:

Australia:

- Fair Work Act 2009 - Governing employment relationships and unfair dismissal protections
- Privacy Act 1988 - Requirements for handling personal information during investigations
- Work Health and Safety Act 2011 - Workplace safety considerations

New Zealand:

- Employment Relations Act 2000 - Good faith obligations, procedural fairness, and dismissal requirements
- Privacy Act 2020 - Protection of personal information during disciplinary processes
- Health and Safety at Work Act 2015 - Workplace safety requirements

International Standards:

- ISO/IEC 27001:2022 Annex A 6.4 - Disciplinary process requirements for information security

4. POLICY STATEMENT

Security Solution Consultants PTY. LTD is committed to maintaining the security, confidentiality, integrity, and availability of its information assets. All individuals with access to organizational systems and data are expected to comply with information security policies and procedures.

Failure to comply with security requirements may result in disciplinary action up to and including termination of employment or contract. All disciplinary actions will be conducted in accordance with principles of natural justice and applicable employment legislation.

5. TRIGGERS FOR DISCIPLINARY ACTION

Disciplinary action may be initiated for, but is not limited to, the following information security violations:

- Unauthorized access to systems, networks, or data
- Sharing or disclosing confidential, proprietary, or sensitive information without authorization
- Breach of information security policies, procedures, or standards
- Failure to follow security procedures or controls
- Misuse of company systems, applications, or resources
- Negligent handling of data, credentials, or security devices
- Introduction of malware, viruses, or other malicious code
- Deliberate bypassing or circumvention of security controls
- Failure to report security incidents or suspected breaches
- Sharing passwords or access credentials with others
- Removal or copying of company data without authorization
- Use of unauthorized software, hardware, or cloud services
- Any other malicious activity that threatens information security

6. PRINCIPLES OF THE DISCIPLINARY PROCESS

All disciplinary actions will be conducted in accordance with the following principles:

6.1 Impartiality

All investigations and disciplinary proceedings will be conducted impartially and without bias. Investigators will be independent of the matter being investigated where reasonably practicable.

6.2 Right to Respond

The individual subject to disciplinary action will be informed of the allegations and given a reasonable opportunity to respond before any decision is made. They have the right to provide their version of events and present any mitigating circumstances.

6.3 Proportionality

Disciplinary actions will be proportionate to the severity of the breach, taking into account factors such as intent, impact, previous conduct, and whether the breach was accidental or deliberate.

6.4 Legal Compliance

All decisions will comply with applicable employment legislation in Australia and New Zealand, including the Fair Work Act 2009 (Australia) and the Employment Relations Act 2000 (New Zealand), ensuring adherence to natural justice and procedural fairness.

6.5 Confidentiality

All disciplinary matters will be treated confidentially and disclosed only to those who need to know for the purposes of the investigation, decision-making, or legal compliance. Personal information will be handled in accordance with privacy legislation.

6.6 Documentation

All stages of the disciplinary process will be documented, including the breach, investigation findings, individual's response, decision rationale, and action taken. Records will be retained in accordance with the Organization's records retention policy.

7. BREACH IDENTIFICATION AND REPORTING

Information security breaches may be identified through:

- Security monitoring and logging systems
- Incident reports
- Internal or external audits
- Management observations
- Employee, contractor, or third-party reports

When a potential breach is identified, it must be reported immediately to the individual's direct manager or supervisor and the CISO (Chief Information Security Officer) or designated Information Security Manager.

8. INVESTIGATION PROCEDURE

8.1 Initial Assessment

Upon receiving a report of a potential breach, the CISO or designated investigator will conduct an initial assessment to determine the nature, severity, and potential impact of the breach.

8.2 Notification to Individual

The individual subject to investigation will be notified in writing of the allegations and the investigation process. In cases of suspected gross misconduct, the individual may be suspended with pay (for employees) pending the investigation outcome.

8.3 Evidence Gathering

The investigator will gather relevant evidence, which may include system logs, access records, emails, documents, witness statements, and any other pertinent information. All evidence will be collected and preserved in accordance with forensic best practices.

8.4 Interview with Individual

The individual will be invited to a meeting to discuss the allegations and provide their response. They have the right to be accompanied by a support person or representative (as permitted by law). The meeting will be documented.

8.5 Investigation Findings

Upon completion of the investigation, the investigator will prepare a report documenting the findings, including whether the allegations are substantiated, partially substantiated, or unsubstantiated. The report will include recommendations for appropriate action.

8.6 Timeline

Investigations will be conducted as promptly as reasonably possible, typically within 10-15 business days, unless the complexity of the matter requires additional time. The individual will be kept informed of any delays.

9. LEVELS OF DISCIPLINARY ACTION

Disciplinary action will be progressive in nature, proportionate to the breach, and will take into account the individual's employment history and any mitigating factors. The following levels of disciplinary action may be applied:

9.1 Verbal Warning

For minor or first-time breaches where the impact is minimal and there is no evidence of malicious intent. The warning will be documented and placed on the individual's file. The individual will be reminded of security obligations and provided with any necessary training or guidance.

9.2 Written Warning

For more serious breaches, repeated minor breaches, or where a verbal warning has not resulted in improvement. The written warning will specify the breach, expected improvements, consequences of further breaches, and a review period (typically 3-6 months).

9.3 Final Written Warning

For serious breaches or failure to improve following previous warnings. The final written warning will clearly state that further breaches may result in termination of employment or contract. It will remain on file for a specified period (typically 6-12 months).

9.4 Suspension

Suspension with or without pay (for employees only) may be applied during the investigation of serious allegations or where the individual's continued access to systems poses a risk to the Organization. For contractors, access may be temporarily suspended during investigation.

9.5 Termination of Employment or Contract

For very serious breaches, gross misconduct, or repeated failures to comply with security requirements despite previous warnings. Termination will be conducted in accordance with applicable employment law and contractual obligations, including notice periods and final payments where applicable.

9.6 Special Provisions for Contractors and Third Parties

For contractors, consultants, and third-party personnel, the progressive discipline process may not apply. Depending on the severity of the breach and contractual terms, immediate contract termination may be exercised for serious security violations. The contract termination process will follow the terms specified in the relevant agreement.

10. GROSS MISCONDUCT

Gross misconduct is conduct so serious that it fundamentally undermines the employment or contractual relationship and may justify immediate termination without notice (subject to legal requirements and contractual obligations).

Examples of gross misconduct in relation to information security include:

- Intentional theft or unauthorized exfiltration of company data, client data, or intellectual property
- Fraud, including falsification of security records or credentials
- Deliberate sabotage of systems, data, or security controls
- Unauthorized disclosure of highly sensitive, confidential, or classified information to external parties
- Deliberately bypassing or disabling critical security controls with malicious intent
- Introduction of malware or ransomware with the intent to cause harm
- Hacking or unauthorized access to systems with criminal intent
- Selling or trading company or client information
- Actions that result in significant financial loss, reputational damage, or legal liability

In cases of suspected gross misconduct, the individual will be suspended (with pay for employees) pending investigation. Following investigation and opportunity to respond, if gross misconduct is substantiated, immediate termination may be applied in accordance with applicable law.

Note: In Australia and New Zealand, summary dismissal for gross misconduct must still comply with fair procedures and may be subject to unfair dismissal claims if not handled properly. Legal advice should be sought before proceeding with summary dismissal.

11. APPEAL PROCESS

Any individual who is subject to disciplinary action has the right to appeal the decision. The appeal process ensures fairness and provides an opportunity for independent review.

11.1 Right to Appeal

An individual may appeal a disciplinary decision on the following grounds:

- The decision was based on incorrect facts or evidence
- The process was unfair or procedurally flawed
- The penalty imposed was disproportionate to the breach

- New evidence has become available that was not considered during the investigation

11.2 Appeal Submission

Appeals must be submitted in writing to the CEO (or designated senior manager) within 5 business days of receiving the disciplinary decision. The appeal should clearly state the grounds for appeal and include any supporting documentation.

11.3 Appeal Review

The appeal will be reviewed by a senior manager or executive who was not involved in the original decision. Where practicable and appropriate, an independent reviewer may be appointed. The review will consider the original evidence, the individual's appeal submissions, and any new information.

11.4 Appeal Hearing

The individual may be invited to an appeal hearing to present their case in person. They have the right to be accompanied by a support person or representative. The hearing will be conducted fairly and documented.

11.5 Appeal Decision

The appeal decision-maker may:

- Uphold the original decision
- Reduce the severity of the penalty
- Overturn the decision
- Order a re-investigation if significant procedural flaws are identified

The appeal decision will be communicated in writing within 10 business days of the appeal hearing (or receipt of written appeal if no hearing is held). The decision of the appeal is final within the Organization's internal processes.

12. LEGAL COMPLIANCE AND NATURAL JUSTICE

This disciplinary process will be applied in accordance with applicable employment legislation in Australia and New Zealand, including but not limited to:

- Fair Work Act 2009 (Australia) - unfair dismissal protections, procedural fairness, and natural justice requirements
- Employment Relations Act 2000 (New Zealand) - good faith obligations, fair and reasonable dismissal requirements, and procedural requirements

The Organization is committed to following principles of natural justice, which include:

- The right to be informed of allegations
- The right to be heard and provide a response
- The right to have decisions made by impartial decision-makers
- The right to representation or support where applicable
- The right to appeal

Where there is uncertainty about the application of this policy or compliance with employment law, legal advice will be sought before proceeding with disciplinary action.

13. ROLES AND RESPONSIBILITIES

Chief Information Security Officer (CISO)

Responsible for overall implementation and oversight of this policy; receiving and assessing security breach reports; coordinating investigations; recommending appropriate disciplinary actions.

Managers and Supervisors

Responsible for identifying and reporting security breaches within their teams; participating in investigations as required; implementing approved disciplinary actions; ensuring team members are aware of security obligations.

Human Resources

Responsible for ensuring compliance with employment legislation; providing advice on disciplinary procedures; maintaining disciplinary records; supporting the appeal process.

Legal Counsel (Internal or External)

Responsible for providing legal advice on complex disciplinary matters; ensuring compliance with employment law; advising on gross misconduct cases and terminations.

All Personnel

Responsible for complying with all information security policies and procedures; reporting suspected security breaches; cooperating with investigations when required.

14. RECORD KEEPING AND PRIVACY

All disciplinary records will be maintained securely and confidentially in accordance with the Organization's records management and privacy policies. Records will include:

- Details of the security breach or policy violation
- Investigation reports and evidence
- Minutes of meetings and interviews
- Individual's responses and submissions
- Disciplinary decision and rationale
- Appeal submissions and outcomes
- Copies of warning letters and termination notices

Records will be retained for the period required by law and organizational policy (typically 7 years in Australia). Personal information will be handled in accordance with the Privacy Act 1988 (Australia) and Privacy Act 2020 (New Zealand).

15. TRAINING AND AWARENESS

All personnel will receive training and awareness on:

- Information security policies and procedures
- Expected security behaviors and responsibilities
- Consequences of security breaches
- The disciplinary process and their rights

Managers and team leads will receive additional training on identifying security breaches, conducting investigations, and implementing this disciplinary process fairly and legally.

16. POLICY REVIEW AND APPROVAL

This policy will be reviewed annually or when:

- There are changes to applicable legislation
- There are significant organizational changes
- ISO 27001 audit findings require updates
- Incidents reveal gaps in the process

The CISO is responsible for initiating the review. Any changes must be approved by the CEO or designated executive and communicated to all personnel.

17. RELATED DOCUMENTS AND POLICIES

- Information Security Policy
- Acceptable Use Policy
- Incident Management Policy
- Access Control Policy
- Code of Conduct
- Employment Contracts and Confidentiality Agreements
- Privacy Policy
- Records Management Policy

18. CONTACT INFORMATION

For questions about this policy or to report security breaches, please contact:

Chief Information Security Officer (CISO)

Email: Info@secsolutionshub.com

Company: Security Solution Consultants PTY. LTD

Headquarters: Sydney, Australia | Regional Office: Auckland, New Zealand

APPROVAL

This Information Security Disciplinary Process has been reviewed and approved by:

Founder/Principal Consultant

Date: February 22, 2026