CHIEF SECURITY OFFICER

PSR | Protective Security Requirements

The Protective Security Requirements (PSR) is a policy framework that provides a risk-based approach for protecting people, information and assets. It sets out requirements related to security governance, along with personnel, physical, and information security.

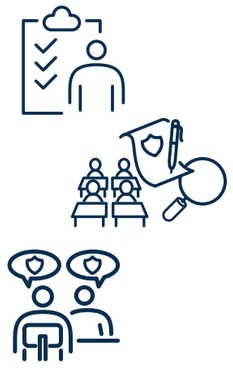
The Chief Security Officer (CSO) exists to ensure that security within an agency is managed at the senior or executive level. You will oversee protective security policy and practice.

The CSO position may be your primary role or a portfolio. While you are not expected to be a technical expert on security matters, it is important you have a direct line to senior leadership on security matters and can provide free and frank advice.

Strengthening security capability and culture should enable your agency to function effectively and better manage your risk. Security is everyone's responsibility, but as CSO, you have additional responsibilities.

Key responsibilities

- Develop and maintain a strategic protective security programme within your agency.
- Implement protective security policy and be responsible for, and ensure compliance with, the policy.
- Maintain oversight of your agency's protective security practices. This includes policy, education and training, and investigations.
- Oversee the development of reporting to monitor protective security capability as part of an annual assurance process.
- Manage and respond to security incidents.
- Liaise with security agencies in relation to protective security.



CSO IN ACTION

Vetting TIAKI

You (or your delegated security team) are responsible for managing security clearance applications in the vetting portal, Tiaki. This includes initiating new and renewal applications, and determining whether any current clearances need to be reviewed.

Contact reporting

Clearance holders within your agency have an obligation to report SOUP (suspicious, ongoing, unusual, or persistent) contact or requests to access your agency's information, assets, or work locations to you. An agency must provide a contact reporting form for clearance holders to complete. You are responsible for receiving these reports and determining the best course of action.

Unauthorised disclosure

An unauthorised disclosure will typically be characterised as a security incident and the resulting investigation should be led by a security function or senior person – with oversight from you. You should receive and action information about this security incident, and record this, along with the outcome of the investigation.

CSO STRATEGIC FORUM

NZSIS hosts a six-monthly CSO Strategic Forum, focusing on system-level protective security trends, policy and strategy. Consistent attendance is encouraged to create continuity and establish a peer network of CSOs. There is a minimum national security clearance requirement for attendance.

www.protectivesecurity.govt.nz
email: psr@protectivesecurity.govt.nz