Elections ACT

ACT ELECTORAL COMMISSION OFFICERS OF THE ACT LEGISLATIVE ASSEMBLY

Protective security policy

Elections ACT

April 2017

Ground Floor, North Building, Civic Square,
180 London Circuit, Canberra City

Phone: 02 6205 0033
PO Box 272, Civic Square ACT 2608

elections@act.gov.au
www.elections.act.gov.au

Accessibility

Elections ACT is committed to making its information and services accessible to as many people as possible.

- If you have difficulty reading a standard printed document and would like to receive this publication in an alternative format – such as large print or audio – please telephone 02 6205 0033.

- If English is not your first language and you require the translating and interpreting service – please telephone 13 14 50.

- If you are deaf or have a hearing impairment or speech impairment, contact us through the National Relay Service:

    - TTY users phone 133 677 then ask for 02 6205 0033
    - Speak and Listen users phone 1300 555 727 then ask for 02 6205 0033
    - Internet relay users connect to NRS (www.relayservice.com.au) and then ask for 02 6205 0033

- ACT Interpreter Service – for the deaf and blind – please telephone 02 6287 4391.

Produced by the
ACT Electoral Commission
PO Box 272, Civic Square ACT 2608.
Phone: 02 6205 0033
Web: www.elections.act.gov.au
Email: elections@act.gov.au

Publication date: April 2017

Contents

Definitions

Term	Definition
ACT Protective Security Policy Framework (ACTPSPF)	Means the Whole of Government security policy that governs the mandatory requirements for all ACT Government Directorates. The Framework is comprised of four sections: • Governance Security: to foster a professional culture ensuring accountability, transparency, efficiency and leadership. • Personnel Security: assessment to ensure that all people employed, including contractors and consultants are suitable and meet high standards of integrity, honesty and tolerance, and hold security clearance to the appropriate level. • Information Security: application of appropriate safeguards to all official information to ensure its confidentiality, integrity, and availability. • Physical Security: physical and procedural measures designed to prevent or mitigate threats or attacks against people, information and physical assets.
Contractor	An individual or company who is engaged under a contractual arrangement to provide goods and/or services to Elections ACT.
Employee	Means a person who is engaged under the *Public Sector Management Act 1994*, or the *Electoral Act 1992* including full-time, part-time, and casual.
Security Governance	The management framework in place to ensure a systematic and coordinated approach to security risk management that focuses on performance.
Security Risk	Any actual or potential threat to personnel, information or assets which requires a coordinated Directorate response.

Purpose

Elections ACT is committed to providing effective protective security programs to ensure the safety of employees and visitors, safeguarding of government assets, official resources and the integrity of sensitive or personal information.

The embedding of protective security as a core element of Elections ACT's planning and approval processes will drive the development of robust and appropriate security risk management strategies in response to a range of security threats.

Elections ACT has implemented a range of integrated policies and procedures that support this policy.

This security policy and any associated, guidelines and/or factsheets were developed to outline mandatory responsibilities and guidance to employees of Elections ACT (including casual

employees and contractors) when considering personal security, security clearances, information security, and building access to ACT Government premises.

The ACT Government Protective Security Policy Framework (PSPF) mandates all directorates to take appropriate measures to protect its people, information and assets. The PSPF outlines the government's overarching protective security mandates. These protective security mandates cover protective security governance, personnel security, information security, and physical security and implementation should be based on a risk assessment.

The PSPF reinforces that directorates are to develop specific protective security policies and implement mandatory requirements and procedures which meet their business needs.

Policy statement

The application of protective security by Elections ACT ensures an operational environment necessary for the confident and secure conduct of Electoral Commission functions and activities.

The ACT Government has implemented the ACT Government Protective Security Policy Framework 2014 (ACTPSPF) which includes 23 mandatory requirements grouped under four sections.

These are:

- Governance security (12 requirements);
- Personnel security (3 requirements);
- Physical security (4 requirements); and
- Information security (4 requirements)

Elections ACT has a responsibility under the ACTPSPF to establish policies and procedures to protect employees, clients, assets and information, and ensure that Elections ACT manages protective security in a consistent manner. The development of documented security policy and procedures provides staff with definitive information on Elections ACT's expectations regarding the management of security risk.

Objective

Elections ACT's Protective Security Policy objectives are to:

- Protect Elections ACT employees and visitors from harm;
- Protect Elections ACT information, assets and infrastructure against:
    - Unauthorised access
    - Malicious damage
    - Theft; or
    - Disruption
- Ensure only persons who are suitable and have an established need are permitted to access official information; and

- Protect the information and assets of other directorates and jurisdictions in accordance with any security agreements and obligations between Elections ACT and those directorates and jurisdictions.

To achieve its security objectives Elections ACT will:

- Apply a systematic and coordinated approach to managing security risks based on the policies and practices outlined in the ACTPSPF, Information Security Manual, and any other legislation and appropriate standards;
- Ensure that planning against security risks forms a part of Elections ACT's culture;
- Ensure that security awareness forms a part of all employee's induction, and ongoing security awareness is included as part of their ongoing training;
- Conduct security reviews and planning that is based on comprehensive, current and reliable information;
- Ensure that protective security related documentation provides treatments that are appropriate to the level of risk and are cost effective; and
- Monitor and assess its operating environment and security treatments on a regular basis.

Roles and responsibilities

Role	Responsibility
Electoral Commissioner	The Electoral Commissioner has overall responsibility for implementing policy and procedures that conform to the ACT Government Protective Security Policy Framework.
Deputy Electoral Commissioner	The Deputy Electoral Commissioner acts as the Agency Security Executive (ASE) and is responsible to the Electoral Commissioner for the ongoing development of Elections ACT's protective security policy and culture and the oversight of protective security matters with Elections ACT. The Deputy Electoral Commissioner also performs the role of Agency Security Advisor (ASA) who is responsible for the day to day performance of the protective security function within Elections ACT.
All staff	All staff are responsible for implementing security policies where appropriate and monitoring their environment to ensure the security of employees and agency information.

Protective security culture

Protective security is most effective when it forms a part of an organisation's leadership behaviours and culture. A strong security culture, based on well established security policies, procedures and practices, with direct and continuing management involvement, is essential to achieving Elections ACT's security objectives.

The Commissioner and Deputy Commissioner play a critical role in demonstrating sound security leadership and promoting a culture based on the premise that the security of Elections ACT staff and information is the responsibility of everyone including casual and contract staff. They do this by ensuring that the process for managing security risk is logical, systematic and forms part of the development of standard business or operational management processes of the individual business unit.

Security risk management and planning

Protective security is about managing security risk and planning its treatment. To be effective, security risk management and planning is to be integrated in to Elections ACT's security culture and day to day business management process and practices.

Good security risk management is based on clear and concise understanding of an organisation's aim, functions and goals and is based on the following principles:

- Security risk management is the business of everyone in Elections ACT;
- Security risk management is part of day-to-day business;
- The process for managing security risks is to be logical and systematic, forming a part of the standard management processes in each business unit; and
- Good security and good business complement each other.

Protection of information

Elections ACT collects and receives information to fulfil its functions and expects all those who access or hold this information to protect it from unauthorised use or accidental modification, loss or release. Staff are expected to do this by:

- Implementing security measures that match the information's value, classification and sensitivity; and
- Adhering to all legal requirements.

Need to know

The basis of 'need-to-know' is one of the underpinning principles in protecting Elections ACT information, and refers to a need to access information based on an operational/business requirement.

Elections ACT employees and contractors should only be accessing and have access to, information which they need to access as part of undertaking their official duties. The 'need-to-know' is not based on a particular classification or positions but on the specifics of the information involved.

Sharing information

Sharing information includes releasing or disseminating information in any form including communicating or corresponding with another person, organisation or entity. In sharing information, both with inside Elections ACT and externally, employees and contractors are only permitted to share information which they are authorised to:

- Have access to; and
- Disclose or release.

In disclosing or releasing information, employees and contractors are also required to ensure that the person, organisation or entity receiving the information:

- Has a right and need to access the information; and
- Is suitable to receive the information, including holding an appropriate security clearance, if required.

Records management

All official information is a valuable asset and resource and must be appropriately managed. Any official information created or used by an employee or contractor must be handled in accordance with the Territory Records Act 2002.

What is official information

Official information is any information which is created, transmitted or stored by:

- An Elections ACT employee as part of executing their official duties;
- A contractor as part of meeting the contract deliverables, working within the Elections ACT environment; and
- An external service provider, acting on behalf of Elections ACT.

There are five subsets of official information, each with different underpinning legislative or policy requirements. The table below shows the different classifications, their definitions and examples.

Classification	Definition
Unclassified	While not strictly a security classification or handling marker, this has been included in this policy in order to allow Elections ACT employees to recognise that some work-related materials do not have any sensitivity relating to their loss or compromise. For example: ▪ information which has been developed for public release. ▪ information, while not intended for public, if disclosure or released would not cause harm, embarrassment or damage to the Commission.
For Official Use Only (FOUO)	This marking is to be used on information when its compromise may cause limited damage to national security, the Electoral Commission, commercial entities, other Directorates, the Assembly or members of the public.

Sensitive: Personal	This marking is to be used for information that contains a fact or opinion, true or not, about an individual or an individual who is reasonably identifiable. This marking is also to be used for information that is defined in the: • ACT Information Privacy Act 2014 as sensitive information including but not limited to: ▪ racial or ethnic origin; or ▪ political opinions; or ▪ membership of a political association; or ▪ religious beliefs or affiliations; or ▪ philosophical beliefs; or ▪ membership of a professional or trade association; or ▪ membership of a trade union; or ▪ sexual orientation or practices; or ▪ criminal record. • Health Records (Privacy and Access) Act 1997 as personal health information which is information: ▪ about an individual's health, an illness or disability; or ▪ collected by a health service provider in relation to the heath, an illness or a disability of the individual.
Sensitive: Legal	This marking is to be used for information that is subject to legal privilege. For example communication between a lawyer and their client made for the principle purpose of: • seeking legal advice/assistance; or • using, or obtaining material for use, in legal proceedings.
Sensitive	This marking is to be used with classified information or unclassified information where: • the secrecy provisions of enactments may apply; and • the disclosure of which may be limited or • prohibited under legislation. For example, Section 222(1) of the Corrections Management Act 2007
Sensitive: Auditor General	This marking can only be applied by the ACT Audit Office to information surrounding the conduct of an audit process.

Sensitive: Cabinet	This marking is to be applied to: • any document including (but not limited to) business lists, minutes, submissions, memoranda and matters without submission that is or has been: ▪ submitted or proposed to be submitted to Cabinet; or ▪ official records of Cabinet. • any other information that would reveal: ▪ the deliberations or decisions of Cabinet; or ▪ matters submitted, or proposed to be submitted to Cabinet. For additional information on the handling of Cabinet information, please refer to the ACT Government Cabinet Handbook.

Protective markings are used to clearly identify privileged and classified information.

It is the responsibility of the author to ensure that official information is appropriately marked. If a marking is required, it is to appear in the header and footer of each document and be clearly visible.

Access to information within ICT Systems

Access to Elections ACT's ICT systems, such as TIGER, is permission controlled to minimise the security risks associated with information loss, theft or corruption; and to safeguard its network.

Employees must only be provided with the minimum system access required to undertaken their official duties.

All users of the ACT Government network in JACS are provided with a unique user identifier consisting of a username and password. This ensures all activities are traceable to individual users.

Employees are personally accountable for their individual usernames and passwords, and must not disclose them to anyone.

Employees must comply with the Acceptable Use of Information Communication Technology Resources Policy.

Storage of official information

Classification	Minimum storage requirement
Unclassified/no protective marking	▪ In accordance with the Territory Records Act 2002 ▪ Documents in folders or filing trays ▪ Files returned to cabinets or secured in locked executive offices. ▪ Computers/laptops logged off at the end of the day ▪ Data storage devices in desks draws, filing cabinets or secure containers

For Official Use Only (FOUO) **Sensitive: Personal** **Sensitive: Legal** **Sensitive** **Sensitive: Auditor General**	▪ Locked Desk Draw ▪ Locked in filing cabinets or secured in locked offices.
Sensitive: Cabinet	In accordance with the ACT Government Cabinet Handbook: ▪ Locked in filing cabinets or secured in locked offices. ▪ Data storage devices in locked cabinets or secure containers.
Protected **and** **Secret**	▪ Class B Storage containers in secure offices ▪ Data storage devices in Class B Containers

Handling of information outside of the office

When taking information out of the office, all Employees are to take reasonable steps to ensure that the information is appropriately protected, as if in the office itself. This including travelling to meetings and other work activities outside of your traditional office environment.

Disposal

Hardcopy information must be disposed of using either a secure (locked) recycling bin or destroyed using a commercial grade shredder.

Large volumes of specific election material such as ballot papers from a previous Legislative Assembly election must be disposed of using a certified secure destruction company. For information on the disposal of large volumes of softcopy information such as this contact the Deputy Electoral Commissioner.

The disposal of information must also be in accordance with the Territory Records Act 2002.

Personnel security

ACT public service employment screening

The purpose of background screening is to assess the identity, integrity and credentials of an Elections ACT's employee or contractor.

As part of the appointment/engagement/recruitment process, all ACT Public Servants, including Elections ACT personnel, undertaking a contracted role are required to:

- Establish their identity by providing 100 points of identification with all documents provided being either originals or certified true copies;
- Undergo a National Police Records Check;
- Undergo a Qualification check, if required for position and requested;
- Provide details of residential address history for the preceding 5 years;
- Complete an ACT Self Disclosure Form; and
- Acknowledge that the unauthorised release of ACT Government Information may be an offence against Crimes Act 1900.

Election casuals and polling officials are not required to undergo employment screening prior to service.

Building access

Building passes permit employees and contractors to access Elections ACT premises and potentially a number of other ACT Government premises.

All building passes are only to be used by the individual to whom they have been issued and be clearly displayed at all times while on ACT Government premises.

Passes remain the property of Elections ACT and must not be used for any reason other than the performance of official duties.

If a building pass is lost, it is the responsibility of the employee to inform the Office Manager who will arrange for the pass to be decommissioned.

Casual employees and contractors

Elections ACT maintains a number of casual employee passes. A temporary pass may be issued where an individual is working for Elections ACT on a casual basis. The register of temporary passes must be completed when a pass is issued and returned.

Access times

Access times for the North Building premises during non-election times for all employees and contractors, are set to a full 24hr, 7 days a week basis.

Access times for election time premises are generally designated in relation to the employees employment status and on a requirement basis. Permanent staff are generally allocated 24hr, 7 days a week access. Other contract and casual staff have access aligned with the span of hours within the current ACT Public Service Administrative and Related Classifications Enterprise Agreement i.e between 7.00am to 7.00pm, Monday to Friday, excluding national and local public holidays.

During election time, employees or their manager may request additional access outside of the normal span of hours, which must be made in writing, approved by the Commissioner.

Keys

The Commissioner and Deputy Electoral Commissioner are to maintain master keys to the office space of the Elections ACT.

During election times, the Electoral Commissioner and Deputy Electoral Commissioner are to maintain master keys and security codes to secure ballot paper storage rooms.

The Material Manager and any other staff member agreed to by the Commissioner may also maintain a key and security codes to secure ballot paper storage rooms with written approval by the Commissioner.

Responding to threatening, abusive or offensive customers or clients

All Elections ACT staff need to be aware and make themselves familiar with of the procedures to follow in the event that they receive a threatening, abusive or offensive client or customer, particularly where there is a threat to an individual's safety or to property.

What to do if you receive a threatening, abusive or offensive phone call

Threatening, abusive or offensive telephone calls are an unfortunate occurrence and can be triggered by a range of circumstances. Usually the calls are directed at whoever answers the telephone, occasionally at a specific person, and sometimes left as a voice message. While it may be very confronting to receive a threatening, abusive or offensive telephone call it is important to maintain your composure, remain calm and professional. Remember, you are in control of the call and you may place the receiver on the desk, move away from the telephone and inform your supervisor of the call.

Calls that threaten life

In rare circumstances, clients or customers may escalate to the point of threats to people or property. All threats are to be taken seriously, and can be in the form of a bomb threat or a chemical, biological or radiological substance, or even a threat of direct physical violence or self harm.

Upon receiving a call in the nature of a threat to life:

- Stay calm;
- Record every word spoken (as best you can);
- Use the attached threat check list to help gather and record details of the call;
- Confirm your understanding of what the caller is saying; ask the caller to repeat the message;
- If the threat is a bomb or other substance (chemical, biological or radiological), ask the caller where the bomb/substance is located, what it looks like and what time the bomb will explode, or when the event will happen;
- If the threat is of physical violence or self harm, ask the caller when and where the action will take place;
- Ask the caller why they are making the threat;
- Listen for any background noise (e.g. cars, trains, planes, music) that may indicate the location of the caller;
- Listen closely to the caller's voice (male or female), voice quality (calm, angry, irrational, intoxicated, well spoken), accent and any speech impediments or mispronunciations;
- Ask the caller to state their name, address and where they are now – they may just tell you this information;
- Do not hang up the telephone when the caller is finished; and

- Complete the threat check list available from http://injacs/documentcentre/Policy%20Documents/Responding%20to%20Threatening,%20Abusive%20or%20Offensive%20Customers%20or%20Clients%20Factsheet.pdf and immediately inform your supervisor, the Building Chief Warden and the Electoral Commissioner and Deputy Electoral Commissioner.

Remember, if there is an imminent risk to the safety of employees, visitors or property, call Triple Zero (000).

Calls that are abusive

On receiving an abusive or offensive telephone call, but where no actual threats of harm are made:

- Stay calm and do not respond in the same manner;
- Tell the caller how their comments make you feel. The caller may be in an emotionally distressed state and unaware of the effect their language/manner is having on you;
- Explain to the caller that if they continue being abusive or using offensive language you will not be able to help them;
- If the caller continues to use abusive or offensive language then tell them you are ending the call;
- Report the matter to your supervisor and the Deputy Electoral Commissioner immediately after you have placed the receiver down.

You should make a record of the time and date of the call, the general message of the call if there is one, and the action you took during the call i.e. “advised the caller if they continued to use offensive language I would end the call, caller persisted with the use of offensive language so I ended the call”.

What to do if you receive a threatening, abusive or offensive client in person

Like difficult telephone calls, there are a range of circumstances that can trigger clients or customers to act in a threatening, abusive or offence manner.

In the event of a customer or client displaying threatening, abusive or offensive behaviour, it is important to attempt to deescalate the situation by:

- Remaining calm and listening closely to understand the problem;
- Not taking the situation personally and remaining courteous; and
- Proposing an action plan/suggest options to solve the issue.

However, if it is not possible to deescalate the situation ensure that you have free egress from the area.

Elections ACT has installed a localised duress alarm. Staff should familiarise themselves with how it functions.

It is important to remember that in any situation, your safety and the safety of others is paramount. If assistance is required due to you or someone else being in immediate danger, call Triple Zero (000).

All situations involving threatening, abusive or offensive clients or customers are to be reported to the Deputy Electoral Commissioner and reported via RiskMan.

Review

This policy will be reviewed every two years or earlier if legislation or process changes occur.

Contact

For further information on the policy, please contact the Deputy Electoral Commissioner