PENRYN
Town Council

INFORMATION SECURITY POLICY

Introduction

In order to operate legally and effectively, the Council must have confidence that its information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Necessary steps must therefore be taken to protect information systems and assets from unauthorized use, modification, disclosure or destruction, whether accidental or intentional. Furthermore, good information security enables us to better achieve the Council's strategic objectives whilst maintaining the trust of our partners and citizens.

Distribution – who needs to be aware of this policy

This policy applies to all staff and all Council information assets. Anyone who processes information for the Council or on our behalf, must either adopt this policy or demonstrate that they have equivalent policies in place.

Context

Background – why this policy is needed

Penryn Town Council (PTC) recognises that information is a valuable resource and seeks to lead and foster a culture that values, protects and uses information for public good. In order to carry out its statutory duties, the Council processes high volumes of information every day. This often includes confidential information about businesses and individuals. Service delivery and business continuity are further dependent on the integrity and continued availability of the Council's systems.

In order to operate legally and effectively the Council must have confidence that its information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Necessary steps must therefore be taken to

protect information systems and assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional. Furthermore, good information security enables us to better achieve the Council's strategic objectives whilst maintaining the trust of our partners and citizens

Objectives – what the policy aims to achieve

This policy is the overarching policy for the Council's Information Security. It sets out the highest level statements of intent by the Council and briefly describes the roles, structures and universal principles required to support these aims.

It is further supported by more detailed policies which prescribe more specific expectations around particular systems or business activities (such as email or mobile working for example).

Scope – what the policy covers

This policy applies to all staff and all Council information assets. Anyone who processes information, for the Council or on our behalf must either adopt this policy or demonstrate that they have equivalent policies in place.

Details

Policy details

In order to protect the availability, integrity and confidentiality of the information under its control, PTC is committed and accountable to principles of Information Security and Assurance.

It is the duty of all staff to proactively uphold the Council's security principles and to understand their own responsibilities.

All breaches of data security, accidental or otherwise, must be reported to the town clerk. Incidents will be investigated where appropriate. Suspected cyber-attacks (including viruses or malicious or otherwise unusual computer activity) must always be reported, in the first instance, to the Town Clerk.

An "information asset" is a collective body of information, defined and managed as a single unit so it can be understood, shared, protected and used effectively.

The Town Clerk is ultimately accountable for all of the assets collected, created, modified by or otherwise processed by staff.

The Town Clerk may delegate operational responsibilities to suitably competent practitioners to ensure that the information assets under their control are handled and managed appropriately. This will include making sure that information assets are properly protected and that their value to the Council and to the public are fully exploited.

Access to information systems must be determined by business requirements. Access shall be granted or arrangements made for users according to their role, only to a level that will allow them to effectively carry out their duties.

The Town Clerk is responsible for ensuring that the Council is kept regularly informed of the most significant information security risks known to face the Council at any given time. The town clerk must understand how the strategic business goals of the Council may be affected by such failures in the secure use of the Council's information systems.

Ongoing consideration of information security is required throughout the system's life cycle, including further risk assessment if the use of the system changes or the data held within the system changes.
The Council will comply with the legislative and regulatory requirements placed on it by outside bodies. These include but may not be limited to:

- The Data Protection Act 1998
- Computer Misuse Act 1990
- General Data protection Regulations
- Payment Card Industry Data Security Standard (PCI DSS)

Breaches and non-compliance

Any breaches of this policy may lead to disciplinary action being taken. Serious breaches of this policy by Council employees will amount to gross misconduct and may result in dismissal.

Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements. If you see a breach of this policy, you must report it to the Town Clerk.

Authority is delegated to the Town Clerk to undertake amendments of an administrative nature as are necessary, or to secure continuing compliance with the law.