

**FALMOUTH AND TRURO
PORT HEALTH AUTHORITY**



IT POLICY

REVIEWED MARCH 2008

1. **INTRODUCTION**

In a business environment, every organisation operates in a climate of risk. It is never possible to remove all risk from an organisation, but it is important to assess and reduce risks to an acceptable level where possible.

Assessing and minimising IT related risks has become increasingly important as dependency on technology increases. As the IT environment changes rapidly and new IT related risks appear, it is vital that staff understand and try to actively control the risk.

This policy will identify and assess the IT related risks that the Authority is exposed to and will set out procedures for reducing these risks and the impact they may have on the Authority's operational procedures.

All of the actions to minimise risks are currently being implemented by the Authority on a day to day basis.

The areas of risk are split into three definitive areas:

- Risks relating to the people using the technology
- Risks relating to the technology being used.
- Risks relating to the way in which the Authority uses the technology.

2. **RISKS RELATING TO PEOPLE USING THE TECHNOLOGY**

The main areas of risk from the people using the technology have been identified as being:

- Unacceptable use by or through staff, partners and former employees (Medium Risk)
- Unauthorised access, fraud and identify theft (Low Risk).
- Loss of key staff (Medium Risk).

The following actions help reduce the potential impact of these risks:

- Make security compliance a priority and enforce it on a regular basis.
- Make sure users keep their passwords secret and implement a policy of not sharing login IDs and passwords.
- Ensure that the Finance & Admin Officer is the only staff member with Administrative privileges on all computers so that vital security settings cannot be changed.
- Educate employees about the dangers of opening email attachments they were not expecting.
- Ensure that all employees know how to identify a security incident, report it adequately and how to react.

3. **RISKS RELATING TO THE TECHNOLOGY BEING USED**

The Authority may be vulnerable to risks relating to the technology it uses. The main technology related risks have been identified as being:

- Breaches in established defences (High Risk).
- Sabotage of data or systems and malicious software (High Risk).
- Computer failure (Medium Risk).

The following actions help reduce the potential impact of these risks:

- Keep up to date checks in place for malicious programs, like viruses and spyware. Screen emails leaving and coming into the Authority's computers. Keep firewalls up to date with a practical schedule of checks and ensure that automatic anti-virus and spyware updates have not been switched off.
- Protect important equipment with surge protectors and uninterruptible power supplies.
- Implement automatic back-ups every day of all computer files onto a removeable storage device. Test that the original information can be retrieved from the back-ups.
- Implement automatic back-ups every day of all computer files onto web space so that all files are retrievable in the event of a fire. Test that the original information can be retrieved from the back-ups.
- Use sufficiently strong passwords and change them regularly.
- Ensure that there are sufficient computers available for general use in the event of failure of one of the systems.

4. **RISKS REATING TO THE WAY THE AUTHORITY USES ITS TECHNOLOGY**

The main process related risks have been identified as:

- Complacency, lack of awareness or understanding of risks or accepting too much risk (Medium Risk).
- Systems lifecycle management (Low Risk)
- Lack of legal and regulatory compliance (Low Risk)

The following actions will help reduce the potential impact of these risks:

- Undertake regular risk analysis of systems.
- Investigate all security incidents and use the information to improve and adapt defences and processes.
- Maintain a complete register of computer assets, including memory and hard disc capabilities. Check all software for legal compliance and cost effective licensing.
- Replace all essential computers on a rolling programme, the most critical equipment being the most technologically advanced.