# Office of Police and Crime Commissioner – Devon & Cornwall
# Policy Cover Sheet

| | |
|---|---|
| **Policy Name:** | Information Security Policy |
| **Version Number:** | V1.0 |
| **Date:** | 4 July 2014 |
| **Policy Author:** | Eleanor Tanner, Office Manager |
| **Policy Authorised by:** | Andrew White, Chief Executive |
| **Policy Sign off Date:** | 25 September 2014 |
| **Policy signed off by:** | Andrew White Chief Executive |
| **EIA status** | Force PIA Assessment 04/12/2013 |

# Office of the Police and Crime Commissioner – Devon & Cornwall Information Security Policy

**Version dated:**4 July 2014

## 1.0 Contents list

## 2.0 Policy Statement [FOIA Open]

2.1 The Office of the Police and Crime Commissioner is committed to the secure use of information, and information technology systems in order to protect the availability, integrity and confidentiality of the information under its control.

2.2 Information is a valuable asset. Business continuity is dependent on its integrity and continued availability. Therefore steps will be taken to protect information assets from unauthorised use, modification, disclosure or destruction whether accidental or intentional.

2.3 The Office of the Police and Crime Commissioner will ensure that it:

- Continually monitors its level of security
- Complies with all applicable legislation, regulations and any other adopted requirements as a minimum. It will comply with government procedures in respect of protectively marked information.
- Implements a risk based approach to information security when assessing and understanding the risks and will use physical, personnel, technical and procedural means to achieve appropriate security measures.
- Takes into account developments in technology and the costs of implementation in order to achieve a level of security appropriate to the nature of the information and the harm which may result from a security breach.

- Assesses the integrity and identity of staff employed by the Police and Crime Commissioner and monitors compliance with their obligations with respect to information security.
- Provides appropriate security education and awareness training to enable all staff to handle and protect information held by the Office of the Police and Crime Commissioner and to carry out their roles in a secure manner.
- Effectively communicates and cooperates with partners and suppliers so that they are aware of and fully understand our security expectations.

## 3.0 Introduction [FOIA Open]

3.1 The Office of the Police and Crime Commissioner's information technology infrastructure is shared with the Devon and Cornwall Police and is therefore jointly required to meet requirements set by the Association of Chief Police Officers (ACPO) for connection to National Police Computer systems. Failure to meet these requirements would impact on the operational use of information, including disconnection from secure networks, and the inability to communicate electronically with partners.

3.2 The provision of effective information security measures will assist the Office of the Police and Crime Commissioner in its compliance with the Data Protection Act 1998 and the application of the Freedom of Information Act 2000.

## 4.0 Procedures [FOIA Open]

4.1 The attainment of this policy will be supported by:

4.1.1 The provision of clear Working Practices on the specific elements of Information Security, accessible through the Police Force Information Assurance Intranet Pages.

4.1.2 The provision of specialist technical advice by the Police Force Information Assurance Unit.

4.1.3 Ongoing liaison between the Office of the Police and Crime Commissioner, the Police Force Information Assurance Unit, the ICT department, and the ICT managed service provider.

4.3 Individual roles and responsibilities:

4.3.1 Following the provision of initial guidance and training, individual members of staff, agency, associated and affiliated workers will be required to comply with the requirements of this policy and associated working practices.

4.3.2 Staff who fail to comply with the requirements of the Policy, Procedures or Working Practices will be assessed in accordance with the OPCC’s Capability Policy and Procedures and if it is determined that non-compliance is a conduct matter, they will be considered for action under disciplinary procedures.

4.4 This policy will be updated in line with relevant changes in legislation, Information Security Standards, connection requirements or other standards.

4.6 The use of all ICT services including all business / operational systems, electronic mail (email), Internet access (surfing), online social media, standalone computers and mobile phones must be in accordance with the Police Force Acceptable Use Policies published on the Police Force corporate intranet - Force Security Policy Site. Failure to observe Police Force Acceptable Use Policies will be considered to be a breach of the Office of the Police and Crime Commissioner’s Information Security Policy.

## 5.0 Audit / Assessment Compliance [FOIA Open]

5.1 This policy has been drafted and audited to comply with the principles of the Human Rights Act. Equality and diversity issues have also been considered to ensure compliance with Equality legislation and policies. In addition Data Protection, Freedom of Information, and Health and Safety issues have been considered. Adherence to this policy will therefore ensure compliance with legislation and internal policies.

## 6.0 Monitoring [FOIA Open]

6.1 Compliance with this policy will be monitored via:

- Incident reporting and escalation procedures
- Data protection audits
- Internal information security audits
- Independent audits

## 7.0 Review and Ownership [FOIA Open]

7.1 The review of the contents of this policy is the responsibility of the Office Manager. Review of the policy will be undertaken annually.

## 8.0 Useful Links [FOIA Open]

- Data Protection Policy
- Information Management Policy
- Information Retention and Disposal Policy
- D338 Police Force Policy -Lawful Business Monitoring
- Police Force Information Assurance Unit Intranet Site