West Lindsey District Council

Information Security Framework

Document Control

Organisation	West Lindsey District Council
Title	Information Security Framework
Author	S M Anderson
Filename	
Owner	Information Governance Officer
Subject	Policy Document
Protective Marking	Not Protectively Marked
Review date	23 Jun 2015

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
21/6/2011	Steve Anderson	Draft V0.1	Branding applied
2/9/2011	Steve Anderson	Draft V0.2	Para 4.3 amended to clarify applicability of training to elected members
29/9/2011	Steve Anderson	Draft V0.3	Adopted by Policy and Resources Committee
6/2/2014	Steve Anderson	Version 1.0	Para 4.3 “Democratic Services” replaced with “Member and Support Services”
23/6/2014	Steve Anderson	Version 2.0	Reviewed by Corporate Information Governance Group. Minor amendments and corrections. Approved by CMT.

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

1 Contents

2 Introduction

2.1 Information is an important asset and of significant value to West Lindsey District Council. Open and transparent government requires us to make information available in many ways. At the same time as providing access to information we must also protect it from threats, internal and external, deliberate or accidental, that could disrupt our work or infringe the rights of staff or customers.

2.2 Information management is about how we create, obtain, process, destroy (or archive) and provide information. How we store the information and how well we understand what we have determines how effectively we can provide it in a variety of ways.

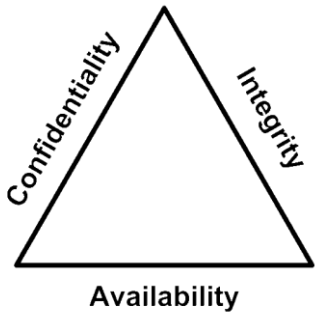
2.3 Information security involves the protection of information for:

2.3.1 **Confidentiality**: Making sure that information is accessible only to those authorised to have access.

2.3.2 **Integrity**: Safeguarding the accuracy and completeness of information and processing methods.

2.3.3 **Availability**: Making sure that authorised users have access to information and associated assets when required.

2.4 The CIA Triad encapsulates in one very simple model everything we need to consider when protecting information. There is a relationship between the elements where a breach of one can affect one or both of the others. For example, if a hacker gains access to some confidential information then it is altogether possible that he/she could change or prevent access to (delete) the information also:



2.5 This document provides a high-level explanation of the framework we use at West Lindsey District Council to secure the information assets we hold.

3 Key Messages

- The council considers its information as one of its most valuable assets.
- The council is committed to open and transparent government.
- The council will protect the confidentiality, integrity and availability of all information in its possession.
- The council will continue to develop effective methods of making its information available.
- The council will maintain an information management and security framework that is “fit for purpose”.
- The council will make sure all staff and members receive regular and effective information security and awareness training.

4 Scope

4.1 This document applies to all information irrespective of format. This includes:

- all corporate information systems;
- all paper records;
- microfiche, visual and photographic materials e.g. CCTV, slides
- spoken conversation, including voicemail and recorded conversations; and
- the technology used to hold, process, transfer and transmit the council’s information e.g. memory sticks.

5 The Framework

5.1 The council is continuously reviewing and organising its information to adapt to legislative changes and changes to customer needs. To this end we are developing a common Information Presentation Layer to collect information from our corporate systems and present it to anyone authorised to see that information though a simple Interface such as a web browser.

5.2 In common with accepted best practice, we employ a layered approach to information security. We protect Information inside a hierarchy of physical, technical and procedural measures as illustrated in the framework model at Appendix 1.

5.2.1 **Physical Security Layer**. All information assets are physically located in secure accommodation. Electronic information is generally stored on servers located in a secure, air-conditioned and fire-protected room. Staff process information in access-controlled offices while paper-based information is stored in lockable storage. Council offices are protected by door access systems that are monitored by Closed

Circuit Television. Staff and members working from home or from remote locations must be provided with appropriate physical security measures. Partners and 3rd parties working as agents of the council are expected to provide the same level of protection for our information as we have.

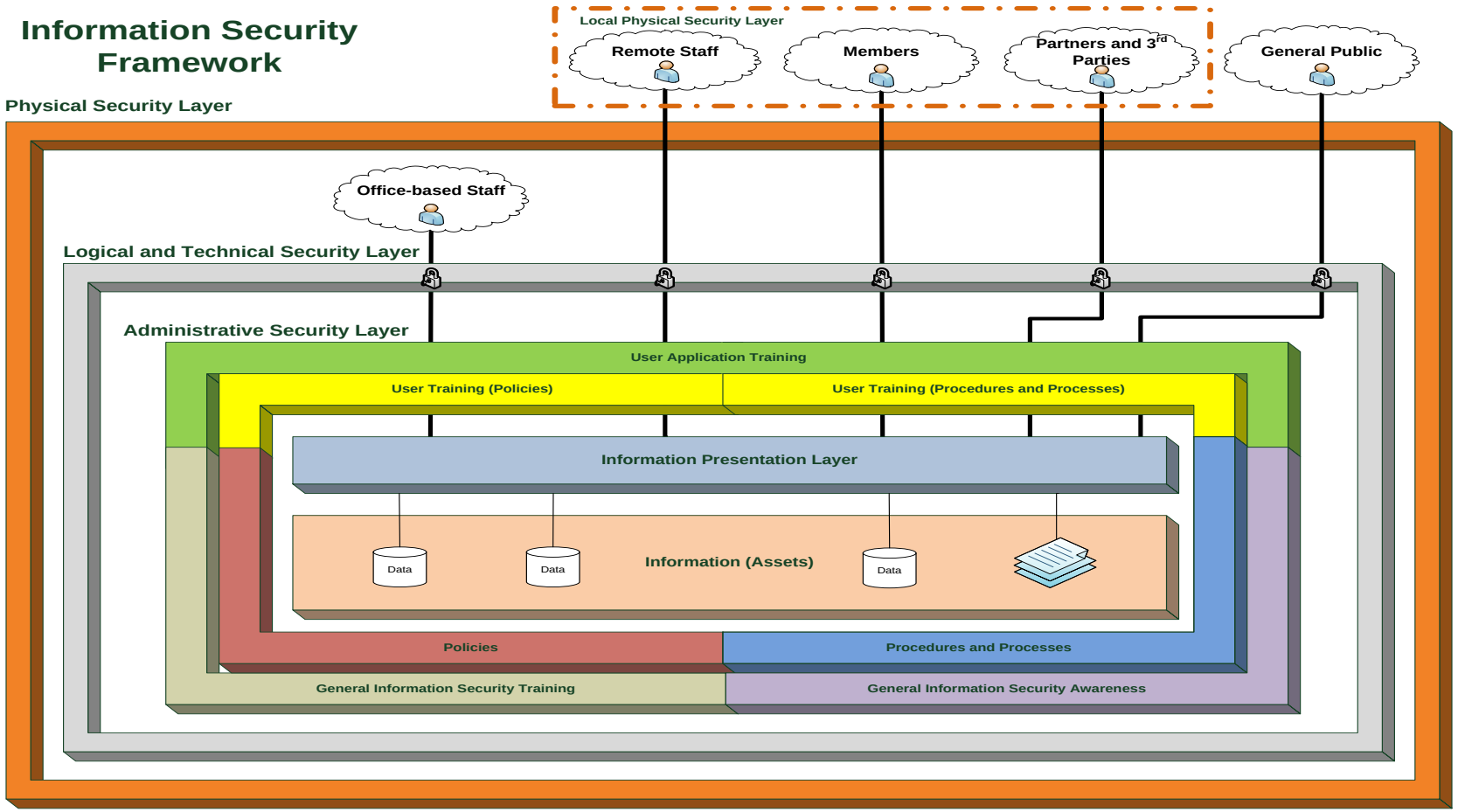
5.2.2 **Logical and Technical Layer**. Controlling access to information and protecting it from a wide range of threats is the job of the logical and technical layer. User accounts and strong passwords, access tokens, anti-virus and backup systems are all examples of the measures organisations need to employ to protect the confidentiality, integrity and availability of its information.

5.2.3 **Administrative Layer**. Often regarded as the most important, the administrative layer is about people, organisational policies, training and security awareness. It is no accident that the framework model shows this as the innermost security layer surrounding our information. All the physical and technical protective measures in the world would be completely ineffective if, for example, a user allows their access credentials to fall into the wrong hands.

5.3 Policies and procedures must be robust and must be backed up by an effective training and security awareness programme. Staff and Members are introduced to this framework in their induction together with some basic security awareness essentials. In addition to reading and signing for the Information Security Policy and supporting policy documents, all staff and elected members with access to the corporate network must complete an online information security awareness training course within one month of their induction. To make sure they have understood the content, the training material includes test questions and staff must stay compliant with the council's Information Security Policy by completing annual refresher training. Members who do not need or want access to the network are strongly encouraged to complete the training for their own development.

5.4 The council keeps security awareness at the top of its agenda using a range of methods. These include publishing a regular articles and messages on the council intranet (Minerva), maintaining a poster campaign, providing awareness refreshers at team meetings and sending broadcast emails to warn of immediate threats.

Appendix 1 – Information Security Framework



West Lindsey District Council

If you would like a copy of this policy in large clear print, audio, Braille or in another language, please telephone **01427 676676**

Guildhall, Marshall's Yard
Gainsborough
Lincolnshire DN21 2NA
Tel: 01427 676676
Fax: 01427 675170

www.west-lindsey.gov.uk