Date: 10th March 2010

Internet Security

REF: H/CICT/2/2010

EXECUTIVE SUMMARY

Context

The purpose of this report is to provide management with assurance that the Council meets the security requirements of the Government Code of Connection. The assessment is a technical and systematic testing and scanning process of the Council's security measures to identify vulnerabilities that could be exploited by individuals attempting to hack in from outside of Council's networks. A separate report refers to the vulnerabilities from individuals who do have authorised access to the Council's networks.

The testing was carried out by NTA Monitor Ltd to highlight and categorise any security issues identified and provide an explanation of the issues raised. NTA Monitor Ltd is an accredited company, commissioned by Welland Internal Audit Consortium to perform the appropriate testing required to comply with the Government Code of Connection. NTA produced a complex and technical report with significant detail which has been reviewed and analysed by the Acting Head of IT and the Consortium to develop an action plan to address the significant issues identified. This report is a summary of the main issues of concern.

Overview

The security scan discovered a number of confirmed security vulnerabilities, as summarised in the table below.
Unconfirmed vulnerabilities are issues known to be associated with the software types and versions the Council is running, none of these were present at the time of the scan.

Severity	Confirmed vulnerabilities	Unconfirmed Vulnerabilities	Total Vulnerabilities
High Risk	0	0	0
Medium risk	4	1	5
Low risk	12	0	12
Informational	5	0	5
Total	**21**	**1**	**22**

Overall NTA's assessment of the Internet security level is **Medium Risk**.

Below follows a summary of the main security issues found during this security scan.

1. Publicly visible internal systems
The Council has some computer systems that are visible from the internet, but do not appear to be designated public internet servers. In general, the Council should only allow external access to internet servers and should block access to all other systems.

As only minor risks have been identified and three recommendations made, the assurance rating following this audit is
GOOD

The recommendations are listed on the action plan.

Scope

The Internet Security - Remote scanning included an examination of the following:

- Registry search and checks
- Internet routing checks
- DNS search and checks
- Internet router checks
- Firewall checks
- Internet server checks
- Other visible system checks

Acknowledgements

The help and co-operation of the Acting Head of IT and the IT Team was much appreciated by the Auditor.

NTA Monitor Ltd

ACTION PLAN

RECOMMENDATION		Priority	Officer Responsible	Agreed Action and completion date
The visible non server hosts identified should be reviewed, and access to them should be blocked where appropriate.		High	Head of Change	**30/9/10**
The table of test findings presented in the detailed NTA report should be used as a checklist for investigation and recording action		Medium	Head of Change	**30/9/10**