Report to: Cabinet Member for Resources

Date: 13th November 2008

Report by: Head of ICT Services

Written by: Nick May, Acting Assistant Head ICT Services
Louise Wilders, Head of Customer Services

E-Government – ICT Security & Ongoing Investment

1. **Purpose of Report**
The purpose of this report is to appraise the Cabinet Member for Resources of the necessity to address a number of ICT Security Risks, the need to upgrade or replace elements of the ICT Infrastructure initially provided as a part of the e.Government programme, and to seek approval to utilise the remaining e.Government Capital Budget to address the most important items.

2. **Recommendations;**
That the following decisions be made –

a) That the Cabinet Member for Resources approve the work required to address the key ICT Security Risks and Oracle System hardware as detailed below funded from the existing e.Government Capital budget:
   - the legislative requirement to connect to the Government Secure Extranet
   - the provision of a Secure Web Mail facility
   - the ICO requirement to encrypt all Laptop Computers
   - the provision of encrypted Digital Storage devices for the transfer of personal information
   - Replacement hardware to support the Oracle Test System

b) The Cabinet Member note that the issue regarding the lack of financial provision to cover the required upgrade or replacement of the e.Gov Corporate ICT Toolsets.

c) The Cabinet Member note that e.Government Capital is now fully utilised

3. **Background**
The e.Government Programme was designed to deliver e.Service delivery on a national basis for all public services. The outcome from a Portsmouth City Council perspective was the provision of a Telephone Contact Centre for all frontline services within PCC (The City Helpdesk), the Corporate Web Site, including the purchase of a Content Management System, Search Engine, etc. which is now hosted by a nationally recognised provider. This included a major exercise to provide the infrastructure to link the City Helpdesk and Web Site to the 'backend' applications, which included the purchase of a CRM.

An implicit part of the e.Government programme was the maintenance of ICT Security, however due to the changing nature of ICT (the internet, e.Mail as a primary source of communication, mobile and flexible working, etc.) the security risks associated with the new technology have been growing at an ever increasing rate and over the last year there have been a number of very high profile data loss incidents which have increased the public perception of this problem.

The e.Government programme had an original capital allocation of £1.888M (funded from £900K of Government grant and £988K of PCC top up). This was supported by an initial revenue budget of £175K however this has been reduced to £109K due to the financial savings process. The remaining e.Government capital budget at the start of 2008/9 was £567K, however, with commitments on outstanding contracts of £54K and a further £150K allocated to undertaking a feasibility study into the Customer Access Strategy, this leaves the budget currently at £363K. [**NB.** It should also be noted that the current e.Government Revenue budget is fully committed to supporting the existing infrastructure.]

4. ICT Security

4.1 Risks

A review of the risks across PCC has identified a number of areas that need urgent attention. The two areas that present the highest level of risk are:

a) The transmission of electronic data to 3rd party partners / organisations.

With the increased need to share information with central government, partners and 3rd party organisations comes the responsibility to ensure all information is transmitted using an acknowledged secure method.

Central Government (DWP and DCSF specifically) have now stipulated that from 31st March 2009 all information flow between these Government departments and Local Authorities will have to be transacted via the Government Connect Secure Extranet (GCSx) this affects our provision of a Housing Benefits Service, Child Services and Payroll. It therefore should be noted that the precedent has been set and that all Government departments will now move use this facility for secure communication with PCC.

There is a further requirement for secure communication with agencies and partners other than Central Government – and therefore the Government Secure Extranet will not be suitable for this purpose. Therefore a separate facility to enable the use of Secure Web Mail will also be needed to meet this requirement.

b) Storage of sensitive information on mobile devices and removable digital media.

Laptop computers, PDAs and other mobile computing devices are necessary tools in the modern office environment. However, these devices are easy to lose or be stolen and although these devices can be physically small they can contain a large amount of confidential

information. The pervasive use of memory sticks to store and transport information (some of which is sensitive) has now become a serious issue. To address this issue PCC will need to acquire a solution to encrypt the hard drives of Laptop Computers, and a means to manage the security of digital media.

4.2 Solutions to address ICT Security Risks

- Transmission of electronic data to 3rd party organisations

(i) The Government Connect Secure Extranet (GCSx) provides a strategic solution (now mandated by DWP, CLG, & DCSF) for secure electronic communication with Central Government and other Local Authorities.
At present PCC is in the process of gaining Code of Connection compliance, however this has required a marked increase in the level of ICT Security across the whole of PCC. To meet these requirements needs significant investment in the ICT Infrastructure to bring it to a minimum level of security including a more restrictive set of ICT Policies with a formal process of enforcement. The current estimate of costs to make PCC compliant is £180K.

(ii) To provide a Secure Web Mail Service, enabling the secure communication with agencies other than Central Government will require the purchase of a service from a 3rd Party Supplier at a cost of £22K.

- Mobile Device and portable digital media encryption

The Criminal Justice and Immigration Act now gives the ICO the power to impose substantial fines an organisation that deliberately or recklessly commits a serious breach of the Data Protection Act, this now includes the loss of information from an unencrypted portable digital device. To address highest risk areas it is recommended that:

(i) The procurement of a tool to enable the encryption of the hard drive of all Laptop Computers at a cost of £111K.

(ii) The provision of encrypted portable digital devices for use by Services that can justify the necessity to copy sensitive / personal information. The budget allocation for this purpose is £30K.

5 Oracle Test System

The hardware supporting the test environment for the Oracle System (which provides the Finance, HR, and Procurement applications) is now obsolete and will no longer be supported by the Supplier. It is therefore necessary to replace this hardware at a cost of £20K.

6 ICT Corporate Toolsets

6.1 Issue

As a result of the e-Government programme and other corporate initiatives a number of Corporate ICT Toolsets were acquired, e.g. the Corporate Website including online self-service facilities, City Help Desk ICT architecture, MS Outlook, the Telephony Switchboard, etc.

The fundamental issue is that no financial provision exists for the enhancement, upgrade or eventual replacement of these tools which now presents an issue to all Services which utilise these tools.

6.2 Facilities Requiring Attention

The corporate tools provided by the original e.Government programme need to be enhanced or in some cases replaced, current areas that need to be addressed with estimated costs:

- Website / IntraLink
  - online forms package (existing facility needs replacement) - £6k
  - search functionality (currently in flight) - £4k
  - Content Management System Review (review/enhance config) - £25k
  - e-booking facility (outstanding requirement) - £50k
  - Maps (currently not useable by public) - £40k
  - e-payments (enhancement) - £15k
  - Web2.0 (new facilities) - £10k

- City Help Desk
  - Voice recording (failed, needs replacing now) - £40k
  - Call Management System upgrade (improved management info) - £40k
  - Workforce Management system (spend to save but dependent on CMS)
  - Reporting for Switchboard (to provide essential reports) £20k*

- CRM – to upgrade and implement (including integrations) £150K – £200K

7. Equalities Impact Assessment

An Equalities Impact Assessment is not necessary in this instance as there is no impact on any of the equality strands, but an Equality Impact Assessment will be completed on the ICT Policies as a consequence of this report.

8. City Solicitor's Comments

The City Solicitor is satisfied that it is within the Council's powers to approve the recommendations as set out.

.....
Nick May
Acting Assistant Head of ICT Services

.....
Louise Wilders
Head of Customer Services

9. **Access to Information**

Background List of documents –
Section 100D of the Local Government Act 1972

The recommendations set out above were approved/approved as amended/deferred/rejected by the Cabinet member for Resources on 13 November 2008.

Signed: ……..