

Taunton Deane Borough Council

Corporate Governance Committee – 20 May 2013

Audit of Data Security Breaches

Report of the Legal and Democratic Services Manager

(This matter is the responsibility of the Leader of the Council)

1. Executive Summary

<p>This report provides a progress update following the audit carried out by South West Audit Partnership on the 15th February 2013. In addition members are asked to approve the Data Security Breach Management policy for implementation.</p>

2. Background

- 2.1 As part of the 2012-13 audit plan a review was undertaken to assess the adequacy of the controls and procedures in place for Data Security Breaches across the Council.
- 2.2 The conclusion of the report gave the Council a partial assurance in relation to the areas that were reviewed and made a number of recommendations. A copy of the audit report is attached at Appendix A.
- 2.3 There were a total of eleven recommendations. Two of those recommendations are a priority 4, four are classed as a priority 3 and 5 are a priority 2.
- 2.4 The implementation date for the majority of the recommendations is the 30th June although two of the recommendations have already been completed.
- 2.5 The majority of the recommendations will all flow from recommendation 1.1(a) which is to develop an Information Security Incident Management Process.
- 2.6 Annexed at Appendix B is a copy of that Management Process which members are asked to approve.

3. Finance comments

- 3.1 There are no financial implications in this report. Although it should be noted that any breach of Data Protection can have a severe financial impact on the Council's finances.

4. Legal comments

- 4.1 There are no legal implications in this report although it is good practice to have a policy in place to manage any such incidents should they occur.

5. Links to Corporate Aims

5.1 There are no links to the corporate aims in this report.

6. Environmental and Community Safety Implications

6.1 There are no implications for the environment or community safety.

7. Equalities impact

7.1 An impact assessment is not required in respect of this report. .

8. Risk management

8.1 The risk of not implementing this policy leaves the Council exposed should there be a breach of data protection.

9. Recommendations

9.1 The Committee is asked to approve the Information Security Incident Management Process and note the report.

Contact

Contact officer: Tonya Meers
Telephone: 01823 358691
E-mail: t.meers@tauntondeane.gov.uk

Taunton Deane Borough Council

► Data Security Breaches

Issued to: Tonya Meers
*Legal & Democratic Services
Manager*

Keith Wiggins
ICT Client Lead

Shirlene Adam
Section 151 Officer

Peter Lappin
Audit Manager

Gerry Cox
Head of Audit Partnership

Working in partnership with



Date of Report: 15 February 2013

Issued by: Neil Roper
Audit Manager

Hayley Pattenden
Lead Auditor

Data Security Breaches

Management Summary

As part of the 2012-13 audit plan a review has been undertaken to assess the adequacy of the controls and procedures in place for Data Security Breaches across the Authority.

The Governance, Fraud and Corruption Audit process focuses primarily on key risks relating to cross cutting areas that are controlled and/or impact at a Corporate rather than Service specific level. It also provides an annual assurance review of areas of the Council that are inherently higher risk. This work will enable SWAP to provide management with assurance that key controls are in place.

SWAP will use the findings of these reviews to support the assurance that is required as part of the Council's Annual Governance Statement; it will also provide assurance to the External Auditor on areas that they have requested specific assurance, such as data quality.

Local authorities face a number of regulations with regards to information security. Perhaps the most significant of these is the Data Protection Act, enforced and overseen by the Information Commissioner's Office (ICO). Since April 2010, the ICO has the power to impose on data controllers, such as local authorities, a civil penalty of up to £500,000 for serious breaches of personal information. Substantial fines, a number exceeding £100,000, have already been imposed on councils for breaches involving personal information and the ICO has proved to be unsympathetic to the difficult financial situation that councils face. Indeed Christopher Graham, the Information Commissioner, commented: *"There is too much of this sort of thing going on across local government. People who handle highly sensitive personal information need to understand the real weight of responsibility that comes with keeping it secure."*

Councils need to ensure that they have effective controls in place to counter data security breaches. These controls should provide a framework for a comprehensive, professional and integrated approach to addressing this issue. An effective framework should include the following three key elements:

- Enforcing an Information Security Strategy that encompasses data classification. *This should ensure that the Council's information assets are surrounded by the appropriate level of security in accordance with this classification.*
- Identifying the possible risks posed by data security breaches and adopting the appropriate measures to counter them.
- Creating and maintaining a strong culture of information security awareness amongst staff.

When the Data Security Breaches audits have concluded at all the reviewed organisations in the partnership we will issue a report to the participants giving an overall view of the arrangements in place.

Summary of Significant Corporate Risks

The following table records the inherent risk (the risk of exposure with no controls in place) and the manager's initial assessment of the risk (the risk exposure on the assumption that the current controls

are operating effectively) captured at the outset of the audit. The final column of the table is the Auditors summary assessment of the risk exposure at Corporate level after the control environment has been tested. All assessments are made against the risk appetite agreed by the SWAP Management Board.

Areas identified as significant corporate risks, i.e. those being assessed as 'high' or 'very high' risk areas in line with the definitions attached should be addressed as a matter of urgency.

Risks	Inherent Risk Assessment	Managers Initial Assessment	Auditors Assessment
Users do not recognise a data security breach when it occurs.	High	Medium	High
Third party discloses council held information that has been shared with them.	High	Low	Low
The organisation fails to report appropriately an information security breach.	High	Medium	High

Summary of Significant Findings

The following were identified as key findings for the service and therefore categorised, in accordance with the definitions attached, as a level '4' or '5' priority in the action plan.

- Central record of information security incidents
- Information Sharing Agreements

Further details of audits' findings can be viewed in the full audit report, which follows this Management Summary.

Conclusion and Audit Opinion

▲★☆☆ Partial

I am able to offer partial assurance in relation to the areas reviewed and the controls found to be in place. Some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

The Council does not have a documented security incident or response plan for data security breaches. Staff are not required to attend mandatory or refresher training on information security and the Council's policy and guidance in these areas. The corporate induction for new staff provides limited information on information security. Staff that had been trained did not know where to access the Council's information security policies and guidance. Additionally, staff were not aware who they should contact and how in the event of a data security breach or what action should be taken.

A significant finding was that the Council do not maintain a central log or record of all information security incidents. It follows that we were unable to locate evidence that any data security breaches had occurred and subsequently been properly investigated and reported to the ICO as necessary. This was highlighted when our work at another local authority identified a theft of client data from a third party that is likely to have included TDBC client data. We believe that this was reported to TDBC but no found no record of this or any action to establish the extent or impact of the incident at TDBC. Additionally, it was unclear whether this had been reported to the ICO.

The Council do have some arrangements in place with third parties that they may share information with. The Model Service Delivery Contract between TDBC and Southwest One makes it clear that Southwest One are data processors in the contract and covers issues such as staff and sub-contractor training.

However there is no specific Information Sharing Agreement between TDBC and South West One that supplements the data protection clause in the contract to address the best practice described in the ICO guidance on information sharing agreements. Whilst Information Sharing Agreements are not a statutory requirement, they should help specify and justify data sharing and the ICO will take this into account should they receive a complaint about the data sharing practices at an authority.

However there are areas of positive practice with regards to data security. The Council have authorised to connect to the GSi / GCF under the GCSx Code of Connection (CoCo). Email Protective Marking (EPM) is now in use across the authority and appropriate staff have GCSx mail accounts. The Council also have an Information Security User Guide in place and a member of the Client Team attends a quarterly Information Security Officers (ISO) Meeting along with South West One and members of SCC Client Team to discuss information security issues.

Detailed Audit Report

Objectives & Risks

The key objective of the service and risks that could impact on the achievement of this objective were discussed and are identified below.

Objective: To ensure that the organisation has in place the appropriate and up to date working practices and procedures to identify, record and respond to information security breaches.

Risks:

- Users do not recognise a data security breach when it occurs.
- Third party discloses council held information that has been shared with them.
- The organisation fails to report appropriately an information security breach.

Method & Scope

This audit has been undertaken using an agreed risk based audit. This means that:

- the objectives and risks are discussed and agreed with management at the outset of the audit;
- the controls established to manage risks are discussed with key staff and relevant documentation reviewed;
- these controls are evaluated to assess whether they are proportionate to the risks and evidence sought to confirm controls are operating effectively;
- at the end of the audit, findings are discussed at a close-out meeting with the main contact and suggestions for improvement are agreed.

The audit was identified in a risk review meeting with the s151 officers of the SWAP client group as one of the common themes across the authorities in the partnership. The scope of the work is to address the following points:

- How are breaches and potential breaches managed?
- Is there a lessons learned process?
- Information security / classification.
- What is public and what's not - how should information be disseminated?
- Member awareness and training.
- Review ICO Reports and IA findings from previous years.

The main emphasis of the work is therefore around information governance, incident reporting and response management arrangements at each authority.

Findings

The following paragraphs detail all findings that warrant the attention of management.

The findings are all grouped under the objective and risk that they relate.

1. Risk: Users do not recognise a data security breach when it occurs.

1.1 The GovConnect Code of Connection requires the connected body to have an information security incident management process. I can confirm that the authority are compliant with the GovConnect Code of Connection however I was unable to confirm that the security incident management process has been documented or if sets out the arrangements to identify, respond to, recover from and follow-up information security incidents.

Without a documented process published to all staff there is a risk that a lack of awareness could lead to information security incidents going unreported and subsequently investigated.

1.1a I recommend that the Monitoring Officer ensures that the authority has a documented Information Security Incident Management Process in place. This should include how information security incidents are identified, responded to, recovered from and followed up and the responsibilities for these.

1.2 We sent a questionnaire to 54 staff working in a range of services that handle personal and sensitive information to capture information about their awareness of security policies, incident reporting, protective marking of information and their views on the effectiveness of training. As at 5 October 2012 only 6 responses had been received, a response rate of 11%.

Whilst it is not possible to draw definitive conclusions from such a small sample the responses we received suggest that:

- Not all staff have received information security training. Nor are staff routinely required to sign an acknowledgement that they have been trained. The respondents who had not been trained did not know how to access the Council's information security policies and guidance, or who and how to contact information security staff and the action to take in respect of security breach.
- Whilst all respondents would apply protective markings to information they handle and pass on to others however few correctly identified the "Restricted" and "Protect" protective markings that are applied to information shared by local and central government agencies. It follows that protectively marked may not be handled appropriately, or information may not appropriately marked.

1.2a I recommend that the Monitoring Officer reviews the information security training provided to ensure that all staff who handle sensitive information are trained, are required to acknowledge receipt of the training and are included in a programme of periodic refresher training.

1.2b I recommend that the Monitoring Officer and ICT Client Lead develop guidance and explanation on the application and use of protective markings to email, documents and

records. This guidance should be included in training materials and made available on the intranet.

- 1.3 The authority have an Information Security User Guide that sets out rules for keeping information secure, security classification, and legislative and policy links. The Guide is available to all staff via the TDBC staff intranet.

The contact details for the Data Protection Officer stated in the guide are out of date. There is a risk that information security incidents or issues could be reported to the wrong person or not be reported.

The advice in the Guide is succinct. For example information classified "Restricted" must be encrypted on portable devices but the guide does not indicate how this should be achieved or how information marked "Protect" should be handled on portable devices.

The Guide gives a version number and date but no version history or indication of who approved the document and when it was approved. There is a risk that the document will not be periodically reviewed and updated if necessary.

- 1.3a I recommend that the ICT Client Lead reviews and amends the Information Security User Guide. This should include updating the name and contact details of the Data Protection Officer for the authority. This should also include a record of the version history of the Guide and a date for the next periodic review.**

- 1.4 There is no regular forum for communication between TDBC and Southwest One (SWOne) on information security issues. SWOne facilitate a quarterly Information Security Officers (ISO) Meeting for all their customers. The TDBC ICT Client Lead attends together with the ICT Client Lead and the Information Governance Officer from Somerset County Council (SCC). The meeting does discuss ICT-related information security issues but this is not a permanent item on the agenda. Data security breaches and any lessons learned from them are not discussed.

Although the ISO meeting is useful in terms of ICT technologically-related issues, it would be useful to have a forum whereby TDBC could meet with both SWOne and SCC to share experiences of data security issues or lessons learned from data security breaches that have occurred within individual organisations. Without this, there is a risk that lessons learned from data security breaches will not be shared and the likelihood of a similar breach occurring again could be heightened.

- 1.4a I recommend that the Security Services Team Manager ensures that ICT Data security is made a permanent item on the agenda of the quarterly Information Security Officers Meeting. This should include sharing any lessons learned from data security breaches at Southwest One's customers.**

- 1.5 Staff attend a Corporate induction day when they join the authority. A 20-minute presentation on data protection issues, the DPA and FOI legislation forms part of this induction. The induction does not appear to include:

- security classification of documents and information although basic guidance is given on how to process and store information
- equipment disposal

- how to identify and report information security incidents.

There is a risk that staff will be unable to identify data security breaches or know how to report a breach if information is not provided during induction training.

1.5a I recommend that the Monitoring Officer ensures that a greater focus is given to data security awareness during induction training. This should include guidance on how to identify and report information security incidents.

1.6 There is no programme of periodic refresher training on information security policies or procedures. Without refresher training or a periodic review of staff awareness there is a risk that staff will not be aware of information security policies or procedures that have been updated. This could lead to an information security incidents remaining undetected and unreported.

However I am able to report that the Clear Desk Policy is effective. A walk-around was performed at the offices after staff had gone home. All office areas checked were found to have clear desks i.e. no confidential or personal data was left in clear view on desks.

1.6a I recommend that the Monitoring Officer liaises with HR to establish a refresher training programme for staff or periodic updates with regards to information security policies and procedures.

2. Risk: Third party discloses council held information that has been shared with them.

2.1 We were initially advised that the Council does not share information with third parties and therefore does not have a practice of creating and monitoring information sharing agreements. Subsequently we were provided with the Information Sharing Agreement between SCC and TDBC for the joint Customer Contact service provided by SWOne. This was signed in 2009 by the Senior Responsible Officer for the SWOne contract for SCC and for TDBC by the then Data Protection Officer.

SWOne provide ICT, Facilities and HR services to the Council and delivering these services involves hosting and processing personal data. There is no information sharing agreement between TDBC and SWOne in respect of the services provided by the SWOne to the Council. Whilst such an agreement is not required by law, the ICO considers them to be good practice. The explanation presented to us is that the Model Service Delivery Contract (MSDC) sets out the responsibilities of the parties with respect to data protection (s 17) and the use of authority data (s 18) and that the organisational and technical controls are described in the Information Security Controls (ISec) document that describes the security services provided by SWOne.

We can confirm that the MSDC sets out the data protection requirements in the terms used by the DPA and includes requirements that SWOne to adhere to the authority's Data Protection and Information Security policies and to train staff and sub-contractors who have access to personal data. However the MSDC does not specify the level of detail outlined in the ICO guidance for an information sharing agreement. For example common rules for retention and deletion of data, a single point of contact and procedure for subject access requests and an explanation or justification of the sharing of data between the two parties.

Without information sharing agreements there is a risk that the Council will be unable to

demonstrate that has considered and recorded the relevant compliance issues. In addition the parties in a service that needs to share information may lack clarity as to the information that should be shared and the information governance arrangements that should apply. Information sharing agreements do not provide legal indemnity however the ICO will take them into account in the event of a disclosure or complaint about information sharing.

2.1a I recommend that the Monitoring Officer reviews existing partnerships, contracts and shared service initiatives to ensure that all those that involve information sharing are identified and the type of data shared and the basis on which it is shared are properly recorded. Furthermore an Information Sharing Agreement template should be prepared for use when personal data is shared.

2.1b I recommend that the Monitoring Officer works with SWOne to create a formal Information Sharing Agreement that extends the information in the Model Service Delivery Contract and ISeC to that outlined in the ICO guidance on data sharing agreements.

3. **Risk:** The organisation fails to report appropriately an information security breach.

3.1 I could find no evidence that TDBC have a documented response procedure for data security procedures.

Without this, there is a risk that staff would be unaware of procedures to follow should a data security breach occur. This could increase the likelihood that a data security breach goes unreported to the Monitoring Officer and, should the incident involve significant personal information, the ICO.

3.1a I recommend that the Monitoring Officer and the ICT Client Lead develop a response plan for information security incidents and publish and promote this to all staff at TDBC. This should describe how and to whom security incidents should be reported and provide those officers responsible for investigating and responding to incidents with process and recording guidance.

3.2 There is no central record of information security incidents maintained by TDBC or by SWOne on behalf of TDBC. Security incidents that involve ICT equipment, such as damage to or loss of devices, are reported to the Service Desk. However the Service Desk do not maintain a central log of such incidents or details of any data loss that may have occurred as a result.

Work at another local authority uncovered a security breach that had occurred which is likely to have involved the loss of TDBC data. A third party contracted this local authority had been broken into and SSDC/TDBC client data had been stolen. This included names, addresses, bailiff reference numbers and Council tenant reference numbers.

The above breach occurred in September 2012 and that data was never recovered. This is still a live breach at the local authority concerned and we were unable to ascertain whether this had been reported to the ICO.

There is a risk that TDBC could be unaware of incidents that occur or the data lost or disclosed in an incident. This could mean that data security breaches involving personal data go unreported to the ICO (Information Commissioner's Office) and the ICO may be more likely to take enforcement action as the lack of a record could be seen as a deficiency in the Council's DPA compliance arrangements.

3.2a I recommend that the Monitoring Officer works with Southwest One to create a central record of information security incidents. The log should record details of the incident, any data lost and any subsequent investigations into the breach.

The log should also record whether the breach has required reporting to external bodies such as the Information Commissioner's Office (ICO) or SW WARP.

The Agreed Action Plan provides a formal record of points arising from this audit and, where appropriate, the action management has agreed to take and the timescale in which the action will be completed. All findings have been given a priority rating between 1 and 5, where 1 is low and 5 is high.

It is these findings that have formed the opinion of the service's control environment that has been reported in the Management Summary.

Data Security Breaches

Confidential

Draft Action Plan

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
<p>Objective: To ensure that the organisation has in place the appropriate and up to date working practices and procedures to identify, record and respond to information security breaches.</p>					
<p>1. Users do not recognise a data security breach when it occurs.</p>					
<p>1.1a Information Security Incident Management Process</p>	<p>I recommend that the Monitoring Officer ensures that the authority has a documented Information Security Incident Management Process in place. This should include how information security incidents are identified, responded to, recovered from and followed up and the responsibilities for these.</p> <p style="text-align: right;"><small>SWAP Ref: 20050</small></p>	<p>3</p>	<p>Agreed. TM will review current documentation & produce a new, easy to use incident Management Process. This will be rolled-out to staff via a Leads meeting, staff team meetings & specific training, as required.</p>	<p>Monitoring Officer</p>	<p>30 June 2013</p>
<p>1.2a Not all staff have received information security training</p>	<p>I recommend that the Monitoring Officer reviews the information security training provided to ensure that all staff who handle sensitive information are trained, are required to acknowledge receipt of the training and are included in a programme of periodic refresher training.</p>	<p>2</p>	<p>Agreed. See actions under 1.1a. The roll-out to Leads & staff will be completed by 30 Jun 2013.</p>	<p>Monitoring Officer</p>	<p>30 Jun 2013</p>

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
	<i>SWAP Ref: 20004</i>				
1.2b Staff do not understand the protective marking scheme	<p>I recommend that the Monitoring Officer and ICT Client Lead develop guidance and explanation on the application and use of protective markings to email, documents and records. This guidance should be included in training materials and made available on the intranet.</p> <p style="text-align: right;"><i>SWAP Ref: 20005</i></p>	3	Agreed.	Monitoring Officer and ICT Client Lead	30 June 2013
1.3a Update to the Information Security User Guide	<p>I recommend that the ICT Client Lead reviews and amends the Information Security User Guide. This should include updating the name and contact details of the Data Protection Officer for the authority. This should also include a record of the version history of the Guide and a date for the next periodic review.</p> <p style="text-align: right;"><i>SWAP Ref: 20046</i></p>	2	Agreed & already completed	ICT Client Lead	Complete
1.4a Information security incidents and practice at Information Security Officers	<p>I recommend that the Security Services Team Manager ensures that ICT Data security is made a permanent item on the agenda</p>	2	Agreed & already completed	Security Services Team Manager	Complete





Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
(ISO) meeting	<p>of the quarterly Information Security Officers Meeting. This should include sharing any lessons learned from data security breaches at SouthwestOne's customers.</p> <p style="text-align: right;"><i>SWAP Ref: 20047</i></p>				
1.5a Induction training information security awareness and incident reporting	<p>I recommend that the Monitoring Officer ensures that a greater focus is given to data security awareness during induction training. This should include guidance on how to identify and report information security incidents.</p> <p style="text-align: right;"><i>SWAP Ref: 20044</i></p>	2	<p>Agreed.</p> <p>Monitoring Officer to pick up as part of the action plan referred to in 1.1a above</p>	Monitoring Officer	30 June 2013
1.6a Refresher training programme or periodic updates for information security practice and incident management	<p>I recommend that the Monitoring Officer liaises with HR to establish a refresher training programme for staff or periodic updates with regards to information security policies and procedures.</p> <p style="text-align: right;"><i>SWAP Ref: 20045</i></p>	2	<p>Agreed.</p> <p>This will be implemented via periodic refresher training at Leads meetings & the provision of specific training as required.</p>	Monitoring Officer	On-going
2. Third party discloses council held information that has been shared with them.					
2.1a Contracts and partnerships	I recommend that the	3	Agreed	Monitoring	30 June 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
that involve information sharing have not been identified and recorded	Monitoring Officer reviews existing partnerships, contracts and shared service initiatives to ensure that all those that involve information sharing are identified and the type of data shared and the basis on which it is shared are properly recorded. Furthermore an Information Sharing Agreement template should be prepared for use when personal data is shared. <i>SWAP Ref: 20048</i>			Officer	
2.1b Personal information stored and processed by Southwest One on behalf of TDBC is not governed by a specific information sharing agreement	I recommend that the Monitoring Officer works with SWOne to create a formal Information Sharing Agreement that extends the information in the Model Service Delivery Contract and ISeC to that outlined in the ICO guidance on data sharing agreements. <i>SWAP Ref: 21077</i>	4	Recommendation understood. However is our view The SWO contract already covers data protection & processing responsibilities in sufficient detail.	Monitoring Officer	N/A
3. The organisation fails to report appropriately an information security breach.					
3.1a Documented response plan for breaches	I recommend that the Monitoring Officer and the ICT Client Lead develop a response	3	Agreed. As in 1.1a TM will review current documentation & produce a	Monitoring Officer and ICT Client Lead	30 June 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
	<p>plan for information security incidents and publish and promote this to all staff at TDBC. This should describe how and to whom security incidents should be reported and provide those officers responsible for investigating and responding to incidents with process and recording guidance.</p> <p style="text-align: right;"><i>SWAP Ref: 20043</i></p>		<p>new, easy to use incident Management Process. This will be rolled-out to staff via a Leads meeting, staff team meetings & specific training, as required.</p>		
<p>3.2a Central record of information security incidents</p>	<p>I recommend that the Monitoring Officer works with Southwest One to create a central record of information security incidents. The log should record details of the incident, any data lost and any subsequent investigations into the breach.</p> <p>The log should also record whether the breach has required reporting to external bodies such as the Information Commissioner's Office (ICO) or SWWARP.</p> <p style="text-align: right;"><i>SWAP Ref: 20049</i></p>	<p>4</p>	<p>Agreed. TM will set up and maintain a central electronic database of security incidents.</p>	<p>Monitoring Officer</p>	<p>30 April 2013</p>

Audit Framework Definitions

Control Assurance Definitions

Substantial		I am able to offer substantial assurance as the areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed.
Reasonable		I am able to offer reasonable assurance as most of the areas reviewed were found to be adequately controlled. Generally risks are well managed but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Partial		I am able to offer Partial assurance in relation to the areas reviewed and the controls found to be in place. Some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
None		I am not able to offer any assurance. The areas reviewed were found to be inadequately controlled. Risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Categorisation Of Recommendations

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors, however, the definitions imply the importance.

Priority 5: Findings that are fundamental to the integrity of the unit's business processes and require the immediate attention of management.

Priority 4: Important findings that need to be resolved by management.

Priority 3: The accuracy of records is at risk and requires attention.

Priority 2: Minor control issues have been identified which nevertheless need to be addressed.

Priority 1: Administrative errors identified that should be corrected. Simple, no-cost measures would serve to enhance an existing control.

Definitions of Corporate Risk

Risk	Reporting Implications
Low	Issues of a minor nature or best practice where some improvement can be made.
Medium	Issues which should be addressed by management in their areas of responsibility.
High	Issues that we consider need to be brought to the attention of senior management.
Very High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.

Appendix B

TAUNTON DEANE BOROUGH COUNCIL

INFORMATION SECURITY

INCIDENT MANAGEMENT PROCESS

Taunton Deane Borough Council
Council Offices
Belvedere Road
Taunton
TA1 1HE

www.tauntondeane.gov.uk

WHAT TO DO IF THERE IS A BREACH OF THE DATA PROTECTION ACT 1998

A POLICY ON INFORMATION SECURITY - INCIDENT MANAGEMENT PROCESS

The Council has a responsibility under the Data Protection Act 1998 (DPA) to ensure appropriate and proportionate security of the personal data it holds. Although the Council takes this duty very seriously there may be an occasion where there is a data security breach. In these circumstances staff should follow the procedure set out below:

1. Immediately notify the Council's Data Protection Officer (DPO) (The Council's Monitoring Officer) or in her absence another member of the Legal Department, you will need to advise the DPO of the nature of the breach i.e. has the data been lost, shared, stolen or unlawfully processed, the amount of data involved, how many people will be affected and the content of the information. You will also need to notify the DPO of any steps you have taken to contain or recover the breach. A Data Protection Breach Response Evaluation Form is annexed to this policy at Appendix A for this purpose.
2. The DPO will then offer advice on any immediate actions that can be taken and commence an investigation. The DPO will also set out a detailed action plan of what should happen next.

The investigation and action plan will deal with the following:

a) Containment and recovery

- Who needs to be made aware of the breach
- Who is needed to assist with the investigation and any containment exercise
- How can the breach be dealt with: can it be contained by simply finding the lost piece of equipment e.g. lost laptop, or access codes changed

- Is there anything that can be done to recover any losses and limit any damage
- Do the police need to be informed

b) Assessing the risks

- What type of data is involved
- How sensitive is the data – some data is sensitive because of its personal nature e.g. medical information whilst other data is sensitive because of what might happen if it was misused e.g. bank account details
- If data has been lost or stolen, are any protections in place such as encryption
- What has happened to the data – if stolen is it possible that its use could be harmful to individuals
- Regardless of what happened to the data what could the data tell a third party about the individual
- How many individuals' personal data are affected by the breach
- Who are the individuals affected
- What harm could come to those individuals
- Are there any wider consequences to the loss
- If the data includes bank details consider contacting the banks as they may be able to assist in preventing fraudulent use

c) Notification of breaches

- Notify the individual(s) affected. If the breach has been contained and the DPO's investigation concluded they should be advised of this. Otherwise they should be informed that an investigation has been commenced and what immediate steps have been taken to contain the situation
- Consider notification to the Information Commissioners Office (see notes below)

- Are there any other bodies that need to be notified

Deciding whether to notify the ICO:

It should be noted that there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, but the Information Commissioner believes serious breaches should be brought to the attention of his Office

There is no definition of a serious breach but the following should assist in deciding whether or not a report should be made:

Potential harm to individuals

Where there is significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, there should be a presumption to report.

Where there is little risk that individuals would suffer significant harm there is no need to report.

Volume of the data involved

There is a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Every case must be considered on its own merits but a reasonable rule of thumb is any collection containing information about 1000 or more individuals should be reported.

However it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high perhaps because of the circumstances of the loss or the extent of information about each individual. If the Council is unsure whether to report or not, then the presumption should be to report.

Sensitivity of the data

There should be a presumption to report to the ICO where smaller amounts of personal data are involved where the release could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is sensitive personal data as defined in section 2 of the DPA. As few as 10 records could be the trigger if the information is particularly sensitive.

Making the report

Where the DPO decides that a report should be made to the ICO it should be done as follows:

By email at: mail@ico.gsi.gov.uk

or by letter to: *Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.*

The notification should include:

- The type of information and number of records
- The circumstances of the loss / release / corruption
- Action taken to minimise / mitigate effect on individuals involved including whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body has been informed and their response
- Remedial action taken to prevent future occurrence
- Any other information you feel may assist us in making an assessment

What will the Information Commissioner's Office do when a breach is reported?

The nature and seriousness of the breach and the adequacy of any remedial action will be assessed and a course of action determined. They may:

- Record the breach and take no further action
- Investigate the circumstances of the breach and any remedial action which could lead to:

- 1) no further action
- 2) a requirement on the data controller to undertake a course of action to prevent further breaches
- 3) formal enforcement action turning such a requirement into a legal obligation

It should be noted that the Information Commissioner does not have the power to impose a fine or other penalty as punishment for a breach. Their powers only extend to imposing obligations as to future conduct.

d) Evaluation and response

- Evaluate the risks and where they lie
- How can the risks be minimised
- Has the breach identified any weaknesses in security measures, how can this be rectified
- Are staff aware of their duties, is further training needed

The investigation and any remedial action should be fully documented and kept centrally by the DPO.

APPENDIX A - Data Protection Breach Response Evaluation Form

Questions	Answers
What is the data?	
How many people are affected?	
Where is the data now and how many people have seen it?	
What is being done to recover the data?	
How did the data loss occur?	
What policies are in place?	
What training/ awareness raising measures have been taken in the light of this episode?	
When did this episode begin?	
Has this happened before?	