MISF Agenda Meeting 44: 19th October 2010

Attendance:

Attended		Attended	
Comm Serv Business Support – Health & Social Care -		CE Communications -	
Corp Supp Contact Centre – Risk Management - Legal – HR – Kim Spry Revs & Bens - Mark Finance - ICT - Richard Woodfield ICT - John Finch		C&YP	
Devon Audit - Devon Audit - Devon Audit -		D&R Service Support - Maintenance –	

Agenda:

1. Apologies
2. Minutes from last meeting
3. Outstanding Actions.
4. Security Incidents
5. Partnership Update
6. Compliance
7. Security Incident reporting process
8. AOB

1. Apologies		
Jane McGuire		
2. Minutes from last meeting		
3. Outstanding Actions	**Actions**	**Who**
Communicate security policy • Net consent policy management software is being decommissioned as maintenance payments have been stopped. It has been unused in the Council for over 3 years, and several thousands of pounds will be saved by not renewing it.		

4. Security Incidents

4.1 Councillors and staff have received phishing emails, which are on the increase nationally, and local councils have been specifically targeted. 5 were reported during September. A communication is being sent out as we need to escalate all instances nationally, so they can gather accurate stats of phishing attempts. It is estimated that 1,000 malicious emails specifically target government networks each month, out of 20,000 that are identified each month.

4.2 A complaint was received about PCH staff accessing revenues systems for unauthorised reasons, and passing information onto 3rd parties. The issue has been dealt with by PCH. PCH are reducing the amount of staff that access PCC systems when they disaggregate in November, from around 80 to 25.

4.3 Local administrator accounts are being reviewed as software is being installed by unauthorised people. Software licensing rules are different for the Council than for home use, for example Google Earth which is free for home use, costs £280 per user per year for council use.

4.4 East Devon Council has had a recent incident where data was leaked via email by an employee that had been made redundant. This is something that could be an issue for many councils in the next few months.

5. Partnerships update

5.1 Devon Security Group

- Protective monitoring workshop conducted in Exeter on 13th October.
    - Protective monitoring concerns the logging of events on ICT systems, their storage and access. It is essential as it is used in investigations to determine what actions have been performed on systems, and by whom. Events include log on and off times, who accessed files in certain area etc. The council has been asked to produce logs for the Police to assist their investigations on several occasions, including the Exeter bombing.
    - During the workshop a minimum set of events to be monitored and logged was determined, which will be used by all SW authorities.

5.2 SW WARP

- 5th October
- BeCrypt demonstrated their Trusted client providing access from Home PCs.
    - BeCrypt have developed a USB device which can be plugged into a home computer and can be used to connect to the Council network over the internet providing full S drive, application and email access. This has been approved for use nationally – but the PCC option follows
- VSRA providing 3G access from laptop, netbook and tablets.
    - A solution using a Vodafone 3g dongle has been tested within the Council, and will allow for full S drive, application and email access over Citrix. It is now available as a service within the Council.

5.3 South West Information Compliance Group

- Data Protection sub group on 20th October 2010 – topic is compliance and ICO intervention

6. Compliance

6. 1 Government Connect (GCSx)

- Workshop in Exeter on 20th October.
- Long term future for GCSx is to move to public sector network, where all public sector organisations will connect on the same network, rather than separate interlinked networks. This will be cheaper for the Council, and more services will be available than currently. E.g. direct NHS connection.

6.2 Payment Card Industry Data Security Standard (PCI DSS)

- Vulnerability scanning has been taking place.
- Options are being reviewed for future of payments service. Capital expenditure is on hold until a decision has been made.

7. Security Incident Reporting Process

- Process refined, see diagram at the end.

8. AOB

8.1 Risk management system for the Council is to include Risk assessment of the information asset use, misuse of non-use.

8.2 Revenues and benefits staff have received data protection training, and as a result are reluctant to share information with other service teams, as they have had to sign a document stating they are responsible for the data they use.

Revs & Bens staff can share with any department internally, as long as there is an audit trail, email provides a useful trail, which states the request, reason for the request (investigation / court), what data is required and date.

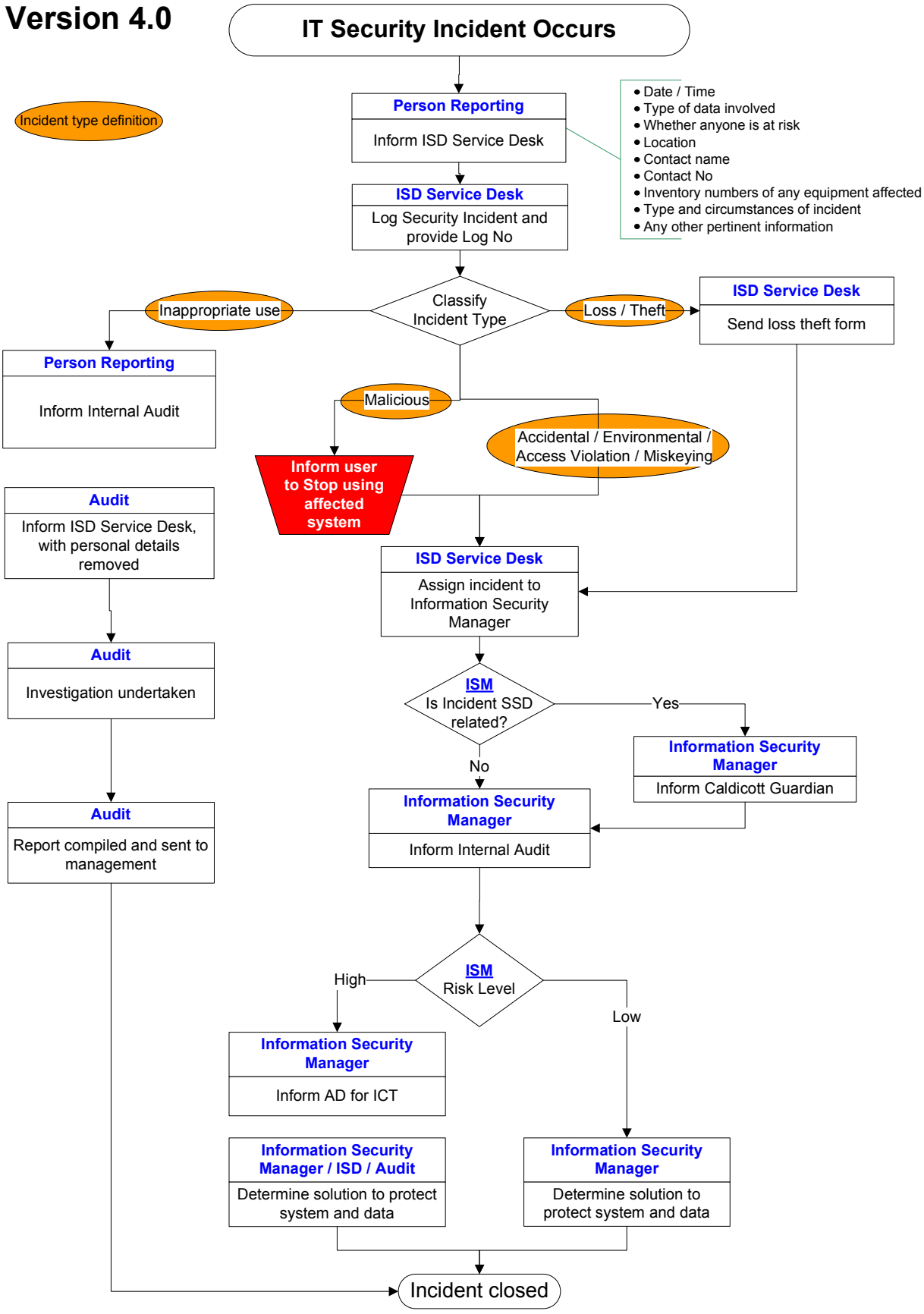
8.3 HR have adopted a grab bag for DR / Business Continuity purposes; in an emergency they can grab, all of their policies, and other essential information. Sensitive data is stored on an Iron Key. One bag is at Windsor, one is at the Civic.

8.4 post meeting staff in HR have stated that it is permissible to download all their work onto a memory stick so as to work at home or away from the office. There is no current PCC Policy allowing work at home.
Only 'NOT PROTECTIVELY MARKED' data and documents can be put on an unencrypted memory stick / disk.
All sensitive data must be put on an Iron Key or transmitted / communicated via an encrypted / secure system.

Security Incident statistics for September

	2010	Jul-10	Aug-10	Sep-10
Malicious				
Data Disclosure	7	2	1	2
Data Manipulation	-			
Denial of Service	-			
Intentional Damage	-			
Social Engineering	14			5
Unauthorised Device Connection	19			
Unauthorised Information Access / use	4			2
Virus / Malware	18	1	5	3
Access Violation				
Access Control Management	1			
Access Control Sharing	4	1	1	
Granting Physical Access	1			
Environment				
Environment Failure	-			
Infrastructure Failure	-			
Natural Damage	-			
Accidental				
Miskeying	-			
Receiving unauthorised information	12	7	3	
Sending information to wrong recipient	-			
Thefts/Loss				
Unencrypted Device	2		2	
Data / Document	-			
Encrypted Device	5	1	1	
School Laptops	2			
School Desktops	-			
Other equipment	4	1	1	
Inappropriate Use				
Unlicensed Software	1			1
Accessing inappropriate material	3		1	
Accessing inappropriate services	2			
Total	**99**	**13**	**15**	**13**

Version 4.0


IT Security Incident Occurs
Incident type definition
Person Reporting
Inform ISD Service Desk
• Date / Time
• Type of data involved
• Whether anyone is at risk
• Location
• Contact name
• Contact No
• Inventory numbers of any equipment affected
• Type and circumstances of incident
• Any other pertinent information
ISD Service Desk
Log Security Incident and provide Log No
Classify Incident Type
Inappropriate use
Loss / Theft
ISD Service Desk
Send loss theft form
Person Reporting
Inform Internal Audit
Malicious
Accidental / Environmental / Access Violation / Miskeying
Inform user to Stop using affected system
Audit
Inform ISD Service Desk, with personal details removed
ISD Service Desk
Assign incident to Information Security Manager
Audit
Investigation undertaken
ISM
Is Incident SSD related?
Yes
No
Information Security Manager
Inform Caldicott Guardian
Audit
Report compiled and sent to management
Information Security Manager
Inform Internal Audit
ISM
Risk Level
High
Low
Information Security Manager
Inform AD for ICT
Information Security Manager / ISD / Audit
Determine solution to protect system and data
Information Security Manager
Determine solution to protect system and data
Incident closed