

AUDIT COMMITTEE 24 JUNE 2010

ANNEX B

External audit report recommendations previously agreed by the Committee.

Report to those charged with Governance: Agreed by Audit Committee 10 November 2009

| Ref | Recommendation | Agreed Yes/No | Proposed Action or reason for disagreement | Responsibility | Timetable for Action |
|-----|---|---------------|---|---------------------------------------|---|
| 1 | <p>SAGE and Network</p> <p>All Sage and Network passwords should:</p> <ul style="list-style-type: none"> • be 6-8 characters in length, and contain at least one number; • have a forced change frequency of 30-60 days; • be disallowed if they have been used in the past 12 times; and • be locked out after three failed attempts. | No | <p>It is accepted that the recommendation represents best practise in password management for systems that are protected by a single authentication method.</p> <p>Sage passwords were compliant with forced change frequency at the time of audit; the password length and history have now been implemented. The Sage system already locks users out after three failed attempts.</p> <p>Network passwords were compliant with password length and change frequency at the time of audit. We will increase the history of changed passwords from 5 to 12. We do not have the granularity to enforce a single numeric; we would need to enforce "complex passwords". Given that we currently receive up to twenty calls per day to the Help Desk relating to users forgetting the network passwords. Most of these are from operational officers and the impact, out of office hours, is to prevent these officers from accessing the systems they need to support effective policing. Increasing password complexity will increase the probability of compromised policing by failure to access systems legitimately.</p> <p>Proposed actions are:</p> <ol style="list-style-type: none"> 1. Increase network password history to 12. 2. Seek funding to implement sign on to systems based on warrant/id card and pin number during financial year 2009/10. 3. Seek funding to implement single sign-on such that warrant/id card credentials passed from network logon to Sage avoiding separate sign on. <p>(2) & (3) above - 18/2/10 Update (Tim Glover) – Funding only available to support confidential / PND workstations</p> | <p>Tim Glover</p> <p>Tom Reynolds</p> | <ol style="list-style-type: none"> 1. Increase network password history to 12 by October 2009. 18/2/10 – UPDATE – ACTION COMPLETED 2. Funding for two factor authentication by April 2010. Implementation by April 2011. 18/2/10 – UPDATE – ACTION ONGOING 13/4/10 – UPDATE – ACTION ONGOING 7/6/10 – UPDATE – ACTION ONGOING (Funding not in place for 2009/10) 3. Funding for single sign on by April 2010. Implementation by April 2011. 18/2/10 – UPDATE – ACTION ONGOING 13/4/10 – UPDATE – ACTION ONGOING 7/6/10 – UPDATE – ACTION ONGOING |

| Ref | Recommendation | Agreed Yes/No | Proposed Action or reason for disagreement | Responsibility | Timetable for Action |
|-----|---|---------------|--|-------------------------------|---|
| | | | 4. If 2 and/or 3 not available, further review of network logons. 16/3/10 Update (Tim Glover) - SAGE is protected by strong passwords as a subsequent stage to the network logon. The concern remains that the use of strong passwords at the network logon may be counter-productive and hinder operational policing and security by either causing an increase in the number of forgotten passwords and an increased likelihood of passwords being written down. We are monitoring regional and national developments which may provide a way forward for card and pin access in 2011. | | (Funding not in place for 2009/10) 4. By April 2010. 13/4/10 – UPDATE – ACTION ONGOING 7/6/10 – UPDATE – ACTION ONGOING |
| 2 | Test restores should be performed on a regular basis, perhaps on a rolling schedule. | Yes | There will be an annual test restore. A previous restore test was successful. 1/3/10 Update (Andrew Dale) – Sage is backed up daily and a scheduled annual test restore is carried out. The last restore was successfully completed and a further test restore is scheduled for w/c 1/3/10 16/3/10 Update (Andrew Dale) - The restore occurred on 4 th March and the “partly successful” statement refers to the fact that with no LEICS domain being present it was impossible to connect and log-on to Sage properly to test the functionality etc. Having said that, the successful database-restore means the data should be intact (but can't be 100% sure until a domain is present). 8/6/10 Update (Andrew Dale) – As the test in March was ‘partially successful’ a re-test is scheduled for June. Other potential developments in respect of auditors recommendations may allow us to implement a separate test and DR environment, whereby recovery tests can be performed more frequently. | Andrew Dale Tim Glover | 31 March 2010. 1/3/10 – UPDATE – ONGOING 14/4/10 – UPDATE – ONGOING (NO CHANGE SINCE 1/3/10) 7/6/10 – UPDATE – Further test scheduled for June 2010 |
| 3. | Sage and Network The Authority should undertake a formal review of user activity and use access on at least a bimonthly | Yes | Network – Review of users will be complete by October 2010. | Tim Glover | 31 October 2010. 3/1/10 - UPDATE - ONGOING 13/4/10 – UPDATE – |

| Ref | Recommendation | Agreed Yes/No | Proposed Action or reason for disagreement | Responsibility | Timetable for Action |
|-----|--|---------------|---|---------------------------------|--|
| | <p>basis to ensure that:</p> <ul style="list-style-type: none"> • access privileges are up to date; • unusual activity such as failed logins and unusual time login are detected; • action is taken to address any risks identified; and • a review should be carried out with immediate effect to remove all inappropriate personnel from the access listing. | | <p>Sage – Functionality to check access privileges/unusual activity is in place for Finance Dept to use as resources permit.</p> <p>Corporate Finance to conduct an immediate review of Sage Users. However, it should be noted that the 'leavers' on payroll are checked against the Sage User list each month.</p> <p>Failed log-ins on Sage can now be logged following the setting change in (1) above.</p> <p>1/3/10 Update (Andrew Dale) - Immediate review was completed and regular monthly review of leavers is taking place.</p> <p>Failed log-ins can be picked up in two ways – (1) if three failed log-ins cause a user account to be locked, Corporate Finance are required to unlock the account and (2) a report is available for a manager user that does not use the "FS1" form set within Sage – the report logs <u>all</u> failed log-ins whether the account was locked or not.</p> | Andrew Dale / Muhammad Patel | <p>ACTION ONGOING 7/6/10 – UPDATE – ACTION ONGOING 30 September 2009.</p> <p>3/1/10 – UPDATE – COMPLETED</p> |
| 4. | <p>Intruder Detection System</p> <p>The Authority should investigate the benefits of having an intruder detection system on the Authority's network.</p> | No | <p>We are currently re-accrediting the network to RESTRICTED. This was considered during this work and it was felt to be unnecessary.</p> <p>However, if there is a view that Sage requires extra protection, we will undertake this investigation and present a business case to consider implementation during 2010/11.</p> <p>16/3/10 Update (Tim Glover) - Funding for intrusion detection was included in the capital programme approved by Police Authority on 9th February 2010. We are currently developing a</p> | Tom Reynolds | <p>March 2010.</p> <p>3/1/10 – UPDATE – ONGOING</p> <p>13/4/10 – UPDATE – ACTION ONGOING</p> |

| Ref | Recommendation | Agreed Yes/No | Proposed Action or reason for disagreement | Responsibility | Timetable for Action |
|-----|----------------|---------------|---|----------------|---|
| | | | <p>resource plan/timeline for delivery of the capital programme as a whole. This will be complete by the end of March after which it will be possible to provide timescales for the implementation of the intrusion detection.</p> <p><i>13/4/10 Update (Tim Glover) – We have scheduled implementation of the network intruder system for 31st December 2010.</i></p> | | 7/6/10 – UPDATE – ACTION ONGOING |

| Ref | Recommendation | Agreed Yes/No | Proposed Action or reason for disagreement | Responsibility | Timetable for Action |
|-----|--|---------------|--|--|--|
| 8 | <p>Oracle Database</p> <ul style="list-style-type: none"> auditing functionality should be enabled; separate environments should exist for production, testing and development; and all security patches should be applied when released following successful testing. | No | <p>There is a restriction in the application that prevents database read/writes being attributed to individual users. We will explore the cost/viability of changing this restriction and enabling auditing at the database level.</p> <p>We do not do development but accept it is best practise to maintain a test environment. We have test environments for the database and application and will explore the costs of creating a separate Oracle environment to enable patching and version changes to be tested.</p> <p><i>27/4/10 Update (Paul Fingleton) - Auditing – Discussed auditing with the suppliers and have come to the conclusion that auditing the oracle database is unlikely to provide any meaningful information. However, the application does produce a system log and we are pursuing an option to develop this into a readable/searchable format. This will provide more targeted information than an oracle audit. Awaiting a decision regarding funding this option.</i></p> <p><i>Separate physical environments - Awaiting costs from our</i></p> | <p>Tim Glover</p> <p><i>Paul Fingleton</i></p> | <p>Under investigation part by PART April 2010.</p> <p>22/4/10 – UPDATE – ACTION ONGOING</p> <p>7/6/10 – UPDATE – Quotations have been received for creation of the separate test Oracle environment & for improvements to the audit trail. Developing business case to seek funding.</p> |

| Ref | Recommendation | Agreed Yes/No | Proposed Action or reason for disagreement | Responsibility | Timetable for Action |
|-----|---|---------------|---|----------------|---|
| | | | <p>supplier to license the Sage software on a development and test server. Costs should be forthcoming in the next week or so, to present to project board to consider funding.</p> <p>Oracle patching - Pending funding of the development and test server, it will allow the application and testing of oracle security patches in a safe environment, prior to release to production</p> | | |
| 10 | <p>Useful Economic Lives</p> <p>The Authority should consider performing a review of assets that have been fully depreciated to residual value and fleet vehicles lives to ensure that assets are given an appropriate useful economic life.</p> | Yes | <p>A review of the assets which have been fully depreciated will be undertaken during 2009/10 to ensure that assets are given an appropriate useful economic life.</p> <p>8/6/10 Update (Ruth Gilbert) – Completed. External Audit will review the work undertaken as part of their audit of the Statement of Accounts. However, it should be noted that the results of the review has not led the Force to amend its depreciation policy.</p> | Ruth Gilbert | <p>30 June 2010.</p> <p>3/1/10 – UPDATE – ONGOING</p> <p>22/4/10 – UPDATE – Ongoing as part of final accounts</p> <p>8/6/10 – UPDATE - Completed</p> |
| 11 | <p>Payroll Reconciliation</p> <p>The Authority should consider introducing a high-level reconciliation between the payroll and general ledger system at year end.</p> | Yes | <p>Consideration will be given to introducing a high level reasonableness check between the payroll and general ledger system at the year end. This will be dependent on being able to extract the data in the required format.</p> | Ruth Gilbert | <p>30 June 2010.</p> <p>3/1/10 – UPDATE – ONGOING</p> <p>22/4/10 – UPDATE – Ongoing as part of final accounts</p> <p>8/6/10 – UPDATE – Ongoing as part of final accounts. Will be completed by 30th June 2010</p> |