INFORMATION SYSTEMS AUDIT – REPORT ADDRESSING SIGNIFICANT MATTER RAISED BY THE OAG

The City of Swan was a participant in the Information Systems Audit Report 2020 - Local Government Entities completed by the Office of the Auditor General (OAG).

In a report issued to the City January 2020, the OAG identified seven significant matters that required attention by the City.

Under section 7.12A (4)(b) of *the Local Government Act 1995*, the City is required to prepare a report addressing any matters identified as significant by the auditor in the audit report, and stating what action the local government has taken or intends to take with respect to each of those matters.

Within 14 days after a local government gives a report to the Minister, the CEO must publish a copy of the report on the local government's official website.

The City takes this matter seriously and to ensure a high standard of due diligence in relation to the management of information systems and controls the City will monitor and track progress of implementation of actions through quarterly progress reporting which will be reported to the Audit Committee.

SIGNIFICANT MATTERS – INFORMATION SYSTEMS AUDIT

1. SYSTEMS

Recommendation: The City should:

- develop and document information security requirements for accessing the application and to inform all individuals of their duties and responsibilities
- update the user registration form to include key information such as access level
- enhance the existing user access provisioning process. The process should adequately cover request, authorisation and management of all accounts within the system. Assigned privileges should be based on the principle of 'least privilege'
- implement regular user access reviews for all key modules, including privileged user accounts and their assigned access privileges. Any accounts that are identified as being no longer required or those which have not accessed the system for an agreed period of time should be appropriately removed or disabled
- regularly review key modules audit log to identify any possible anomalies or suspicious behaviour
- harden the application security and processes to address known vulnerabilities in a timely manner.

Management Comment: The OAG findings are not unexpected given that the HR/Payroll system (TechnologyOne OneCouncil) has only been operational for a year and many processes and procedures are still being reworked. Security and technical configurations are still being refined also. Changes to the Technology security configuration will need to be carefully prioritised and coordinated with affected Business Units.

Agreed Action: Management will develop and implement process improvements with regards to authorisation and regular review to ensure appropriateness of current and future access to this application. Technical reviews will also be

conducted to harden system access to improve the application's protection level. Multiple improvements have been enacted to this new system since the time of the review, further consultation with the technology vendor will be undertaken to further strengthen system defences.

Responsible Person: Chief Executive Officer

2. USER ACCESS MANAGEMENT

Recommendation: Based on an assessment of risk, the City should:

- enhance the application access and privilege management process to ensure the allocation of access rights and privileges are appropriately requested, authorised and formally recorded
- review current access roles and permissions to ensure appropriate segregation of duties and alignment to business needs. Privileges should be allocated to individuals on the minimum requirements for their functional role
- make sure users are assigned unique user names (IDs) to enforce responsibility and accountability for their actions. If the use of generic accounts is required, it should be appropriately controlled and monitored
- review access and privilege granted to all users to ensure access and privileges rights are appropriate and still required. This should include the review of accounts that have not used the system for an extended period.

Management Comment: The OAG findings are not unexpected given that the Pathway system is earmarked for decommissioning with TechnologyOne. Pathway's sub-optimal security model has been in place for many years, substantially changing the configuration was deferred given the risk to the system's operations when a new system was imminent. Changes to the Pathway system access will need to be carefully prioritised and coordinated with affected Business Units.

Agreed Action: Management will develop and implement process improvements with regards to authorisation and regular review to ensure appropriateness of current and future access to this application. The use of generic accounts will be analysed in conjunction with business units to identify possible alternative arrangements or process changes. It should be noted that this particular system is due for replacement in the next two years, and many security model shortcomings will be addressed with the new system's security model.

Responsible Person: Chief Executive Officer

3. DATABASE SECURITY

Recommendation: The City should:

- document and implement an appropriate database management process to ensure all database accounts are formally requested, approved and assigned privileges are based on the principle of 'least privilege'
- perform regular review of all database accounts to verify that access and privileges are appropriate and still required
- enforce password policy requirements to all database accounts
- implement proactive independent logging and monitoring of database security logs to identify any unauthorised modifications or malicious activity in a timely manner.
- ensure updates to address known vulnerabilities are applied in a timely manner
- improve database hardening based on relevant industry good practice guidelines.

Management Comment: The OAG have highlighted vulnerabilities at the backend of the system to which only system administrators have access and Management believes only advanced hackers could exploit. However tightening privileged access, hardening security configuration, patching, and checking logs are all good practice and the City will investigate the most effective options prior to implementing any changes.

Agreed Action: Security controls will be defined for the Pathway database and current access will be reviewed. Future access will be controlled through creation of improved work instructions and guidelines, reinforced with regular access checks. Technical improvements will be undertaken in conjunction with the software vendor's best practices to tighten security access controls and reduce vulnerabilities.

Responsible Person: Chief Executive Officer

4. INFRINGEMENTS

Recommendation: Based on an assessment of risk, the City should:

- define and document guidelines to inform officers about their duties and responsibilities (e.g. legal, regulatory, City's own requirements) when issuing infringements and using the system
- document and enhance the process to manage infringement books, including the reconciliation of pages that were skipped or cancelled. Regularly review the allocation of books to ensure they are assigned to current staff
- develop a process to proactively identify and refund overpayments
- based on a risk assessment, improve monitoring controls.

Management Comment: There are two key documents which assist in guiding officers in decision making regarding infringements these consist of 'POL-M-154 Enforcement' and the 'Infringement Withdrawal Guidelines'. To complement these documents there are also process maps 'Enforcement Administration' and 'Withdrawal of Infringements', further to these for each category of enforcement there is also a process map which identifies relevant legislation and considerations regulations related to the offence, for example there is a process map regarding a Dog Attack investigation under the Dog Act, this provides guidance on investigation considerations and enforcement outcomes More detailed work instructions related to Community Safety processes are continuing to be developed to provide greater written detail on legal, regulatory and City requirements.

'POL-M-154 Enforcement' was reviewed in early 2019, it should have been sent to the City Executive for endorsement at the time, changes to the policy were limited in comparison to the previous version, the updated policy will now be sent to the Executive Management Team for endorsement. In regards to the finding that operational staff were not aware that 'POL-M-154 Enforcement' exists, it is managements understanding that only one City officer was engaged in the infringement review discussion from Community Safety, in this officers role they are not required as part of their core function to utilise 'POL-M-154 Enforcement' they are required to follow the 'Infringement Withdrawal Guidelines.'

In regards to manual infringement processes, the majority of the Community Safety teams infringements are issued using the electronic pin force system, it's agreed that the manual infringement system should be replaced with pin force or similar electronic infringement system for improved accountability however the risks regarding manual infringement book management are viewed as low due to the low number of manual infringements however will be reviewed.

From the identified overpayments these seem to have primarily occurred when the City payment system changed to Bpoint from Bpay (systems were unable to talk to each other), the City has now reverted to Bpay, it has also been identified that a report can be developed to check on overpayments however this would need to be actioned across the City

Agreed Action: A review of the enforcement policy and relating processes will be conducted. New processes will be considered and current processes updated to ensure clarity on legal, regulatory and City requirements as per the recommendations.

Responsible Person: Chief Executive Officer

5. APPLICATION SECURITY

Recommendation: The City should:

- document and implement appropriate security practices to manage the email system
- improve the email system security configuration and access requirements
- perform vulnerability scans to identify security weaknesses and apply relevant security updates (patches) to remediate vulnerabilities in a timely manner
- proactively monitor system logs to identify unauthorised access or malicious type activity

Management Comment: The OAG have highlighted vulnerabilities at the backend of the email system that only advanced hackers would be able to exploit. However tightening the security configuration, patching, and checking logs are all good practice and the City will investigate the most effective options prior to implementing any changes.

Agreed Action: The email system's security practices will be reviewed, documented, and improved as per the recommendations.

Responsible Person: Chief Executive Officer

6. FIREWALL MANAGEMENT

Recommendation: The City should:

- document and implement procedures to appropriately manage security devices
- implement a regular review process of the firewall configuration. The risk of any accepted exception should be appropriately recorded
- ensure the use of the shared generic administrator account is restricted for only those tasks that specifically require this level of access. For all other tasks, IT staff should be assigned individual user accounts with appropriate privileges for firewall administration
- develop a process to review key security events. Suitable records of these reviews must be maintained
- regularly backup the firewall configuration and test the backups

Management Comment: Managements believes that only advanced hackers would be targeting these vulnerabilities and exposures. However tightening and reviewing the security configuration, patching, and checking logs are all good practice and the City will investigate the most effective options prior to implementing any changes.

Agreed Action: Processes and practices to be reviewed, documented, and strengthened as per the recommendations.

Responsible Person: Chief Executive Officer

7. VULNERABILITY MANAGEMENT

Recommendation: The City should:

- develop and implement an effective vulnerability management process to ensure all relevant 'known' security vulnerabilities are regularly identified. Following successful testing, relevant actions and updates should be applied in a timely manner
- appropriately record decisions (along with any mitigations) made to not address any known vulnerabilities
- implement network segregation between critical systems and user groups
- implement a process to proactively identify unauthorised or unmanaged devices that are attached to the network environment
- monitor Internet access activity and develop appropriate reports for follow up actions.

Management Comment: The OAG's scans of the City's network have indicated some areas for improvement with regards to keeping all system up to date and secured with recommended settings. Software is being acquired to assist with performing the task of identifying non-compliant systems on the City's network and a prioritised list of systems requiring remediation will be developed.

Agreed Action: A process to manage vulnerabilities and monitor devices and access will be developed as per the recommendations.

Responsible Person: Chief Executive Officer