CONFIDENTIAL

Note: Confidential Provisions released on 03/02/2021

Port Augusta
CITY COUNCIL

REPORT FOR:	**Audit Committee**		
MEETING DATE:	20 October 2020		
REPORT FROM:	Director City Services		
REPORT TITLE:	**Cyber Security Work Plan**		
FILE NAME:	F20/204	RECORD NO:	AR20/51060

STRATEGIC DIRECTIONS	
5	**Governance and Financial Sustainability**
5.5	We meet or exceed legislative and accreditation requirements for all relevant programs.

SUMMARY/ABSTRACT

Following the finalisation of the Audit Report from the Auditor General Cyber Security Audit, and a subsequent Cyber Security Audit by Local Government Risk Services, a Cyber Security Work plan has been developed to addresses the items identified within the audits. The purpose of this report is to provide the Audit Committee with a copy of the Work Plan, including an update on the actions completed by Council.

RECOMMENDATION

Audit Committee recommends Council receives and notes the report (AR20/51060) dated 14/10/2020, submitted by the Director City Services in relation to the Cyber Security Work Plan.

BACKGROUND

In December 2019 Port Augusta City Council was one of three Councils randomly selected to be subject to an Audit for 'Examination of the cyber security within Local Government' by the State Government Auditor General, under the Public Finance and Audit Act 1987. The audit was undertaken between December 2019 and February 2020. Reports were provided to the Audit Committee with progress of the audit process, in February and May 2020. The outcome of the Audit was presented in a final draft report in August 2020.

Council participated in a complimentary Cyber Security Audit, funded by Local Government Risk Services, and delivered by consultants CQR. This Audit was undertaken in July 2020, with the final report provided in August 2020.

DISCUSSION

Auditor General Report

The completed report will be submitted to Parliament later in the year. The Auditor General has requested that all information in relation to the Audit is to be retained in confidence until such time as the final report is tabled in Parliament. The 16 findings made as a part of this report have been included within the Cyber Security Work Plan, as attached.

LGRS / CQR Report
Council participated in a complimentary Cyber Security Audit with the final report provided in August 2020. This focussed on testing and 'breaching' our external perimeter to visualise a level of maturity against the industry cyber security benchmarks set by the Australian Signals Directorate. There were no breaches to Council's systems during the testing, however areas for improvement have been identified. The final report for this Audit has not been attached to this report as it details the external vulnerabilities of Council's IT systems, in technical detail, which should not be made public. The findings of the Audit have been summarised within the Cyber Security Work Plan, together with the actions to be taken to address the issues identified.

Cyber Security Work Plan
The actions within the work plan have been scheduled to ensure that they are addressed with the required priority, whilst maintaining the ability of the Information Services team to deliver and monitor everyday ICT requirements and other identified system and procedural improvements. The work plan is attached for reference.

CONFIDENTIALITY PROVISIONS

The Council is satisfied that, pursuant to Section 90(3)(j) of the Act, the information to be received, discussed or considered in relation to this Agenda Item is information the disclosure of which would divulge information provided on a confidential basis by a public authority - Auditor General. It is considered that the open discussion in relation to the Audit, the disclosure of which would breach the Council's obligation to maintain confidentiality, should be considered under confidential provisions.

In addition, the disclosure of this information would, on balance, be contrary to the public interest. The public interest in public access to the meeting has been balanced against the public interest in the continued non-disclosure of the information. The benefit to the public at large resulting from withholding the information outweighs the benefit to it of disclosure of the information. The Council is satisfied that the principle that the meeting be conducted in a place open to the public has been outweighed in the circumstances because the disclosure of the Audit information may severely prejudice Council's Cyber Security and breach confidentiality requirements imposed by a public authority.

Having considered this agenda item in confidence under Section 90(2) and (3)(j) of the Local Government Act 1999, the Council, pursuant to Section 91(7) of that Act orders that report (AR20/51060), discussions and minutes be retained in confidence for a period of 12 months or until such time as advice is received from the Auditor General that the information can be released, and that this order be reviewed every 12 months.

RISK MANAGEMENT

1: Financial/Budget/Asset Management

Council's Information Systems budget includes provisions for the ongoing security, maintenance and upgrade of Council's IT systems and applications.

2: Legal/Policy

The Auditor-General conducted this examination under section 32(1)(a) of Public Finance and Audit Act 1987.

3: Environment/Planning

Not applicable.

4: Community

Council is committed to ensuring the security of all electronic systems and applications, to ensure the ongoing provision of services to the community, and to protect the personal information held within those systems.

Melissa Kretschmer
14/10/2020

Cyber Security Work Plan 2020/2021

Findings – Auditor General	Council Comments	Action	Timeframe
Gaps in cyber security related policies and procedures	Implemented password parameters for all users and drafted an Information Technology General Security Policy	Implement Password Parameters	Completed March 2020
		Information Technology General Security Policy	31 December 2020
Lack of cyber security awareness	The Council has user awareness materials published regularly on the intranet, and has provided LGRS funded Fraud and Cyber Awareness Training in 2020.	Monthly Cyber Security Awareness in Council eNewsletter and on Intranet	Monthly
		Cyber Security Training for all staff	Completed February 2020
Insufficient management of risks and contracts over third party service providers	Tender processes require the provision of relevant risk based information. Contractors are monitored to meet service delivery KPIs. LGA also monitor contractors.	Clauses to be included within template Request for Tender and Contract documentation	31 December 2020
ICT related risk register and reporting does not exist	Corporate Risk Register monitors general ICT risks. An ICT Risk Register will be developed.	Corporate Risk Register to be updated	31 March 2021
		ICT Risk Register to be developed	30 June 2021
Lack of evidence of ongoing ICT security audits, penetration testing or vulnerability assessments	Draft ICT policy includes programmed penetration testing. Undertake basic information security reviews and testing as part of the implementation or upgrade of any systems.	Undertake Penetration Testing every 2 years and report outcomes to Audit Committee	Completed July 2020
		Information Technology General Security Policy	31 December 2020
Weakness in password controls	Password controls have been implemented, a password cracking attempt is scheduled for June to ensure compliance and enhanced security has been achieved.	Implement Password Parameters	Completed March 2020
		Password cracking undertaken to ensure compliance	Completed June 2020

Findings – Auditor General	Council Comments	Action	Timeframe
Weakness in privileged user access management practices	All elevated privileged user accounts have been reviewed with some deleted. Privileges have been revised for vendors and modified to the minimum privileges required.	Undertake review of privileged user accounts	Completed March 2020
		Implement stronger password controls for privileged user accounts	Completed June 2020
Insufficient user access management policy, procedure and practices	All 5 users identified had left Council in the last 6 months, and accounts terminated within 4 months. Accounts are maintained to ensure record keeping and service provision.	Information Technology General Security Policy	31 December 2020
Privileged user security events were not logged or monitored	Log and monitor privileged account usage commenced. Review and monitoring of security events from privileged account usage as a part of the auditing of privileged user accounts procedure.	Information Technology General Security Policy	31 December 2020
		Added to Information Technology General Security Policy	31 December 2020
Security updates not regularly installed	Server patching is controlled internally and vendor application patches are tested before being implemented.	Information Technology General Security Policy	31 December 2020
Physical access to the server room is not appropriately restricted	Not enough space to provide a locked server room. The DR and secondary server are in locked and controlled areas.	Identify alternative location for server room, or enhance security arrangements	30 June 2021
Insufficient network segmentation	Only 1 computer failed to meet requirements, due to the IT team and others using the computer and room for testing.	Review network segmentation as part of the Network infrastructure upgrade.	31 December 2021
Insufficient end-user device security	ASD's Windows hardening high and medium priority recommendations have been adopted and included in the draft ICT Policy.	Information Technology General Security Policy	31 December 2020

Findings – Auditor General	Council Comments	Action	Timeframe
Insufficient change management protocols	Systems 'updates' are managed by ICT and vendor staff and documented within Vendors project plans. Also addressed in draft ICT Policy.	Information Technology General Security Policy Patches to be evaluated in a small number of systems before full deployment.	31 December 2020
No backup policy and procedure, disaster recovery plan and associated testing	This has been included in the draft ICT Security Policy. DR site is a full backup of the primary environment. The upgraded system will incorporate a new full DR site, and offsite backup media storage for secondary recovery.	Information Technology General Security Policy	31 December 2020
		New DR site and off-site backup storage to be established.	31 March 2021
Information security incident response plans have not been established	Council has a business continuity plan, which includes an action plan for non-critical ICT functions and a Critical Function Sub Plan. The plans for all Council business units also incorporate ICT system recovery for the particular business units. Council has also developed a Records Management Disaster Plan.	Cyber and Digital Security Breach Policy	31 March 2021

Findings – CQR Audit	Council Comments	Action	Timeframe
Outdated and unsupported software (High)	The new operating system reports its web service 'versioning' very differently and reported as out-of-date. Council is running the latest version.	No action required as Operating System updates will bring reporting back into line with previous versions.	Completed July 2020
SMTP server facilitate email spoofing (High)	Remediation underway - DMARC based email verification system in final testing phase	Implement email verification system	31 December 2020
Externally exposed administrative interfaces (Moderate)	This service was the email Administration interface including the Web based email. Interface whilst 'displayed' cannot be logged into.	Service URL changed to be internal only and externally URL points to OWA login.	Completed June 2020.
Potentially dangerous services accessible over the internet (Moderate)	The services noted have been mitigated and 'hardening' note added to internal server build notes.	Services have been blocked by network access control lists (ACL's).	Completed June 2020.
Remote VPN supports IKE aggressive mode (Low)	This is deemed to be a very low risk.	This will be addressed and mitigated in the Network infrastructure upgrade.	31 December 2021
SSL and TLS vulnerabilities including weak ciphers (Low)	Some of these services are vendor services. All services have been identified and a remedial process commenced.	Notified vendors and remediation processes underway. Internal servers checked for vulnerabilities.	31 December 2020
Webservers lack protective HTTP headers (Low)	These webservers are vendor controlled but Council hosted.	Vendor notified of CQR outcome and vendor responded with immediate action to rectify.	Completed August 2020
Server version and IP address information is disclosed (Information)	All externally facing servers have been checked including webservers. Council considers this to be very low risk but acknowledges the noting.	This information has been blocked.	Completed August 2020
Facilitation of denial of service attacks (Information)	No action required as DoS and DDoS attacks cannot be stopped.	Current monitoring ensures DDoS attacks are detected as quickly as possible to enable rapid response.	Completed July 2020