Action Plan - Cyber Security Strategy Update January 2023

ID	Area	Observation	Action - quick win	Action - longer term	% Complete
AP - 1	Defend / Technology	Maintain firewall and scanning services.	Maintenance of current infrastructure and services.	Migration to virtual firewall to enhance functionality and management.	67%
AP - 2	Defend / Technology	Maintenance of end-point protection for devices – Anti Virus, USB Encryption and Mobile Device Management.	Maintenance of current endpoint protection.	Consolodation of endpoint protections as part of planned move to enhanced Microsoft licencing	50%
AP - 3	Defend / Technology	Undertake Cyber Security Health Checks and Penetration Testing.	Maintain the programme of quaterly vulnerability scans of the server suite and rolling programme of workstation scans.	Establish schedule of independent health checks.	33%
AP - 4	Defend / Technology	Utilisation of the National Cyber Security Centre tools. WebCheck and Mail Check.	Migration to MyNCSC platform and configuration of services	Exploitation of enhanced features available within MyNCSC	67%
AP - 5	Defend / Governance	Meet compliance regimes which require good Cyber Hygiene (Public Service Network Code of Connection, Cyber Essentials).	Maintain current compliance with Public Service Network and Cyber Essentails.	Development work to move to Gov.Pay platform to harmonise payment processing on secure government platform. Extension of current Cyber Essentials into Cyber Essentials Plus and Cyber Essentials Governance	33%
AP - 6	Defend / Governance	Be an active member of the public sector cyber security community. Participation in the Cyber Security Information Sharing Partnership (CiSP) and Wales Local Authority Warning, Advice and Reporting Point.	Expansion of Welsh WARP membership to include relevant internal stakeholders	Active presence in wider cyber community events	67%
AP - 7	Deter / Technology	Users with wide ranging or extensive system privilege shall not use their highly privileged accounts for high-risk functions.	Identification and remediation of less secure authentication. Expansion of seperation of duties - privileged accounts used solely for adminstrative functions	Review of standard accounts with enhanced privieges.	50%
AP - 8	Deter / Technology	Reconcile current systems in place and last times these were reviewed.	Identiy high risk systems and undertake a scoping review to provide an interim assessment.	Scheduled annual review of existing systems to be setup and ongoing identification and creation of new guidance.	25%
AP - 9	Deter / Technology	Protect enterprise technology by working with specialist partners to develop model architecture.		Where necessary engage consultants with specialist expertise to advise on specific areas while internal capacity is being developed	0%
AP - 10	Deter / Technology	Multi-factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services.	Implemented as a requirement in all new systems	Review of existing systems to identify where MFA is not in place but can be in order to address these.	50%
AP - 11	Deter / Governance	Embed the Secure by Design principle throughout.	Regular Digital Team 'Stand Ups' raising awareness of workstreams and providing a coherent approach to bridge until Solutions Board in place.	Full initiation of Solutions Board to ensure all development follows the Target Operating Model, including Secure by Design and Privacy by Design	50%
AP - 12	Deter / Governance	Review vendor management to address supply chain risk.	Refine current process of System Assessments and IG processes for Third Party management.	Development of NPT Supply Chain Strategy and associated policy and process/procedure.	50%
AP - 13	Deter / Governance	Review (update where appropriate) policies and procedures.	Body of work required to review and update (new posts filled etc)	Scheduled annual review to be setup	33%
AP - 14	Develop / Technology	Explore Active Cyber Defence tools and new technologies to ensure we have the best solutions to match to threats.	Adopt Protected DNS toolkit and EmailCheck into current suite of Active Cyber Defence Tools.	Identify and test further ACDT with a view to implementing into the digital estate.	50%
AP - 15	Develop / Technology	Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises.	Engage in funded "Excercise in a box" opportunity.	Develop a scheduled programme of internal exercises.	33%

ID	Area	Observation	Action - quick win	Action - longer term	% Complete
AP - 16	Develop / Governance	Provide relevant cyber security training for staff and elected members to help detect, deter and defend against the cyber threats.	Report on current statistics of staff e-learning compliance. Awareness of Member e-learning to be raised and completion reported on. High Risk areas to be identified and proactively added to training cycle to address any gaps.	Regular reporting process put in place to collect and report on training compliance levels.	71%
AP - 17	Develop / Governance	Develop and maintain a risk management framework, internal controls and governance mechanisms. Process, procedures and controls to manage changes in cyber threat level and vulnerabilities.	Formalise current processes which provide security governance.	Gap analysis leading to implementation of an Information Security Management System.	25%
AP - 18	Develop / Governance	Aligned with best practice, develop a minimum requirement for all systems used, audit trails, deletion of data etc.	Utilise current critera for System Assessments and IG processes to create a baseline set of requirements.	Develop a standalone internal minimum requirements standard to form part of suite of standards within the Information Security Management System.	50%
AP - 19	Develop / Governance	Develop a communication plan in the event of an incident, which includes notifying the senior accountable individuals, the communication team, statutory notification bodies and relevant external organisation and law enforcement as applicable.	Utilise RACI Matrix from Cyber Incident Response Plan to inform interim communications plan alongs side exisitng reporting mechanisms for statutory bodies.	Expand interim communication plan to include other existing communication plans to formalised cyber incident communication plan.	67%
AP - 20	Develop / Governance	Develop an incident response and management plan, with clearly defined actions, roles and responsibilities.	Incident Response Plan is in place. Review and update of current incident playbooks.	Annual Review of Cyber Incident Response Plan.	100%
AP - 21	Develop - Governance	Create a cyber-specific Business Continuity Management Plan and/or review our Incident Plan to include emergency planning for cyber-attack.	Inclusion of cyber in current Business Continuity Management Plan	Develop separate Cyber Business Continuity Management Plan	50%