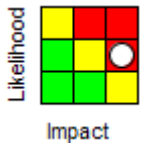
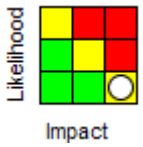
Cyber Risks

Generated on: 24 May 2021

Risk Code	CR62	Risk Title	Cyber Risks
Risk Owner	Jo Dufficy	Updated By	Vic Godfrey
Year Identified	2014	Council Objective	Be a welcoming, inclusive, and efficient council
Risk Description	**As a result of:** - Computer virus - Malware - Ransomware - Computer hacking - Action by Staff/Member (e.g. opening a malicious link) - Malicious tampering of computer records - Information being sent to the wrong recipient - Loss or damage to server room **There is a risk of:** - Systems being interrupted or damaged - Data being corrupted or erased - Personal data being stolen - Breach of the Data Protection Act 2018		
Opportunities	- Safe and effective use of Information Technology		
Consequences	The consequences of these risks include: - Loss of reputation - Ability to provide services is disrupted - Revenue streams are reduced - Additional costs to investigate and test following repair/restoration - Claims for compensation if a third party suffers a financial loss - Fines from the Information Commissioner		
Work Completed	- Information Security policy in place, which applies to staff and Members use of IT systems - Email encryption software (EGress) implemented - Introduced new software (Clearswift and Bloggs) to enhance the checking of threats attempting to attack via the firewall - All data centres have fire suppressing systems and are located in secure areas - Disaster recovery in place at a remote site (Unit 3) - Basic computer insurance provides limited cover for damage to equipment and reinstatement of data (although it does not cover payment of any fines or compensation to third parties) - Business Continuity Plans in place - Ransomware attack resulting in the write-off of IT hardware and infrastructure identified as a financial risk for 2019/20 and 2020/21 (Low/£200k) - Data Protection/FOI SIAS internal audit - Controls in place to ensure any third party providers adhere to NHDC security requirements - Annual PEN Test completed autumn 2018 and PSN Accreditation renewed January 2019 - SIAS audit of Cyber Security (March 2018) provided Moderate overall assurance - Implemented specific cyber roles/responsibilities within the ICT team to strengthen resources and approach (September 2018) - Implemented the recommendations from the SIAS audit of Cyber Security - Reviewed findings of the 2018 penetration test and worked through the minor improvements identified - In 2019, the requirement for Members to be registered as Data Controllers with the ICO was removed		

	- SIAS audit of Cyber Security (August 2019) provided Satisfactory overall assurance and the report made five recommendations (four medium priority and one low priority) - NHDC PSN submission was sent to the Cabinet Office on 19 April 2020 - NHDC received its PSN Compliance certificate in September 2020 - All security patches for Firewalls reviewed and updated, and an in-house penetration test carried out to ensure all links into the corporate network are secure - ICT Manager attended a Cyber Fraud webinar hosted by the London Fraud Forum on 22 April 2021
Ongoing Work	Business-as-Usual Activities - Anti-virus/malware software in place and automatic updates are performed to servers and all PCs/laptops/tablets - Email Filter monitoring - Web Filter monitoring - Firewalls continually reviewed and updated - Reviewing firewall log files - Continuing to ensure the latest software security packages are installed and deployed across all firewalls - Microsoft patches kept up to date - Software patches continue to be applied to ensure we are on the latest versions and that security is at the highest levels possible - Annual Penetration (PEN) Tests undertaken and PSN Accreditation renewed to ensure security is at the highest levels - Regular advice and reminders issued to users - LMS training available (e.g. annual DPA 2018) - Control/security systems enable potential threats to be identified, investigated and managed accordingly - Regular reminders to all staff and Members are sent by the Service Director - Customers about the need to be vigilant about opening emails from unknown sources - Attending MHCLG Cyber Pathfinder Training Scheme events (currently being delivered online) - Two Officers with specific cyber security responsibilities, which was implemented following a SIAS audit recommendation Specific (SMART) Actions - Implementing the recommendations from the SIAS audit of Cyber Security (August 2019), including the forthcoming release of a new Cyber Security mandatory training package (review of the training package has taken place and the ICT Manager is working with the L&D Team to get this launched via the Learning Management System (LMS) - estimated launch date September 2021) ~~***Implementation of recommendations and date of training launch to be confirmed with VG on 17 May 2021***~~ - NHDC has met and will be inviting an external Cyber Security Specialist in to carry out Cyber Essentials and then Cyber Essentials Plus, which cannot happen until we return to normal day-to-day working and into the offices (estimated date for this will be late summer 2021)
Current Overall Risk Score	8

Current Impact Score	3	**Current Likelihood Score**	2
Current Risk Matrix		**Target Risk Matrix**	
Date Reviewed	22-Apr-2021	**Next Review Date**	22-Jul-2021
Latest Notes	24-May-2021 On 19 May 2021, the Risk Management Group agreed that the current risk score of 8 was appropriate and the current target score of 6 should be retained at this time. 13-May-2021 Risk reviewed and updated by Vic Godfrey on 22 April 2021. No change made to the risk score. Target risk score (currently 6) to be discussed further with Vic Godfrey on 17 May 2021 prior to May's Risk Management Group meeting.		