Cybersecurity

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	7		
Paper number	[AGC (07/10/2015) 467 DM]		
Meeting date	7 October 2015		
Author	David Moysen, Head of IT		
Output:			
For information or decision?	Information and comment.		
Recommendation	AGC is asked to note the HFEA's Cybersecurity posture		
Resource implications			
Implementation date			
Organisational risk	☐ Low	☐ Medium	☐ High
Annexes			

1. Introduction

1.1. Cybersecurity is a key concern for Government. To that end, CESG have produced clear guidance on the controls that should be in place in every organisation to mitigate the threat of Cyber-attack ("The 10 Steps to Cyber Security"). This paper outlines how the HFEA has addressed the issues raised in the guidance.

2. The Ten Steps

2.1. Information Risk Management Regime

The HFEA has a rigorous Information Risk Management Regime. There are formal SIRO and Caldicott Guardian roles and Information assurance is over seen by CMG with delegated responsibility for implementation and improvement by the Information Governance Group. The Information Security Policy is in line with the standards required by ISO27001.

2.2. Secure configuration

The HFEA actively maintains the secure configuration of IT systems. Patches are applied to software and systems as and when they are released. Regular vulnerability scans are run against systems to identify any potential issues that need to be addressed and users are prevented from making any systems changes.

2.3. Network security

Network traffic is restricted by limiting access only to services required by the HFEA for business use. Multiple firewalls are in place to isolate trusted and untrusted networks and all the firewall rules are based on whitelist principles. Antivirus and malware checking systems are deployed on inbound and outbound routes as well as being installed on local machines and host systems.

2.4. Managing user privileges

User accounts are created when joining the organisation and inactivated when staff leave. Passwords are required to be complex and changed on a regular basis. Remote access to HFEA systems requires the use of token based multi factor authentication. Users are only provided with the security privileges that their roles demand and user access to sensitive data is logged.

2.5. User education and awareness

The Information Security Policy clearly defines acceptable use of HFEA systems and also defines security procedures that are applicable to all HFEA business roles and processes. New starters are made aware of the obligation to comply with security policies and all logins require acknowledgment of the policies. Alerts are sent out to staff if there are relevant security threats and all staff are required to take online security awareness training.

2.6. Incident management

The security policy documents the HFEA's incident management process. Daily offsite backups are made and regularly tested to ensure that data recovery available.

2.7. Malware prevention

Anti-malware solutions are deployed across the HFEA and staff are made aware of specific threats and malicious websites are blacklisted.

2.8. Monitoring

HFEA systems are performance monitored continuously. All access to sensitive information is logged in detail and periodically review for suspicious activity.

2.9. Removable media controls

Removable media is used to transport information as a last resort if secure electronic channels are not available. Encrypted storage devices are provided to HFEA staff for this purpose. If data needs to be sent using cd/dvd then the media device is securely encrypted and the encryption key sent to the recipient by alternate secure channels.

2.10. Home and mobile working

Home and mobile workers have policies and guidance in place to govern how they work remotely from the office. Staff laptops are encrypted and access to remote services is provided by a secure virtual private network.