DYFED ARCHAEOLOGICAL TRUST

CYBER SECURITY POLICY AND PROCEDURES

ymddiriedolaeth archaeolegol
DYFED
archaeological trust

Current since: 2018

Adopted at the Management Committee [board] Meeting of: 23 January 2020

Date of review following first adoption: 31 December 2023

Revised following review:

Re-adopted at the Management Committee [board] Meeting of:

Date of review following re-adoption:

DYFED ARCHAEOLOGICAL TRUST (‘DAT’)

CYBER SECURITY POLICY AND PROCEDURES

Overview

In the course of carrying out its various functions and activities DAT relies on various forms of information technology. It is thus vulnerable from malicious agencies intent on disrupting the work of DAT or corrupting data generated and held by DAT. It is important that all members of staff are aware of the risks of a cyber-attack and the potential consequences of such an attack.

Scope and Purpose

The purpose of this Policy is to provide an organisation-wide framework to ensure that the risk of a cyber-attack is minimised and that if an attack does occur then procedures are in place to ensure minimal disruption to DAT and minimal loss of data.

Information Technology Support

Information technology (IT) support is provided by an external contractor with a good reputation and good track record of providing such support. The external contractor is responsible for setting up DAT’s servers, desk-top PCs and related hardware and software. They install required firewalls and maintain and monitor DAT’s malware and virus checking software. It is DAT policy that no member of staff is able to disable server firewalls and related high-level security systems.

Boundary Firewalls and Internet Gateways

All firewalls etc are installed and maintained by DAT’s external IT contractor. Open ports and services on firewalls will be authorised by DAT’s Chief Executive or Office Manager and approved by DAT’s external IT contractor. Open ports no longer required will be closed. It is DAT’s policy to have only those open ports and services that are essential to DAT’s business.

Secure Configuration

New desk-top PCs and laptops are purchased through DAT’s external IT contractor and set-up by them.

DAT’s external IT contractor has full administrative rights over desk-top PCs.

If new software is required a request must be made to DAT’s Administrative Assistant. This request must be authorised by DAT’s Chief Executive or Office Manager. Software installation will be done by DAT’s external IT contractor.

User accounts are reviewed on a monthly cycle by DAT’s Administrative Assistant or Office Manager and unnecessary accounts deleted. If an account is required for a new employee or a volunteer then then a project manager or above must put in a request a least a week before it is required and its level of permission discussed and authorised by DAT’s Chief Executive or Office Manager. DAT’s external IT contractor will create the account.

Passwords must be of at least nine characters and contains at least one of: lower case character, upper case character, number, special character. Users will be prompted monthly to change their password. Users must completely change their passwords, not just one or two characters of an old password. Sharing of passwords is not permitted.

All unnecessary software is removed from desk-top PCs and laptops. DAT’s Administrative Assistant reviews software requirements on a 3-monthly programme and removes unnecessary software.

AutoRun/AutoPlay is disabled from all desk-top PCs.

Use of mobile media

Mobile media is an easy way by which malware can be transferred from device to device, and so it is DAT's policy to restrict their use in order to minimise risk.

Data sticks should ideally be previously unused, and if not must be virus checked immediately on plugging into a desk-top PC. On no account must a visitor to DAT use a data stick on DAT's desk-top PCs. The safe use of data sticks on laptops is provided below.

External hard drives are not permitted, unless authorised by DAT's Chief Executive or Office Manager.

CDs and DVDs are a relatively safe method of data transfer. It is essential that DVDs and CDs are virus checked immediately on insertion into a desk-top PC or laptop.

It is permitted to download data from digital cameras, survey equipment and similar data collection devices.

Internet Access

It is DAT's policy to restrict web browsing to work-related tasks. Malware can enter DAT's systems through web browsing and downloading files. Before visiting a previously unvisited website or revisiting a site after a period of time the URL of the website must be virus checked using a URL provided to all staff. All downloaded files must be virus checked before they are opened. Untrusted websites must not be visited.

Visiting social media sites such as Facebook is not permitted, unless authorised by DAT's Chief Executive or Office Manager. Accessing private email accounts, such as Hotmail, gmail etc is not permitted. The use of Dropbox, Office 365 and similar data transfer programmes is not permitted, unless authorised by DAT's Chief Executive or Office Manager.

Virus Checking

DAT has virus detection software in place which is regularly updated and monitored by DAT's external IT contractor. All members of staff should run a manual virus scan on a weekly basis. DAT's administrative staff must be informed immediately if the virus checking software is not running correctly, or if it has detected a problem.

WiFi Access

In order to minimise risk, the WiFi uses a separate IP address from DAT's main server. Use of WiFi is limited to those members of staff who require it for work purposes. It is not available for visitors to DAT.

Email

DAT's Microsoft Outlook is the only permitted email system. Incoming emails are 'washed' by an external provider. Pop up-messages alerting the user to a new incoming email have been disabled. Emails from an untrusted source should not be open and must be deleted. On no account must an attachment be opened from an untrusted source.

Laptops

Laptops are potential source of virus infection, and therefore their use is carefully monitored. Laptops are used for talks and presentations and therefore it is inevitable that USB data sticks are plugged into them. To minimise risk a laptop must be booked out using DAT's booking system and on return it will be virus checked by DAT's Administrative Assistant. It is not permitted to book it out unless it has been virus checked. It is not permitted to connect laptops directly to DAT's server.

Visitor access

Visitors to DAT wishing to view digital data must use a dedicated desk-top PC. This provides access to data on the hard-drive but no access to DAT's servers.

Remote access to the Server

Remote access to the server is not permitted, unless authorised by DAT's Chief Executive or Office Manager.

If a security breach is suspected

If a member of staff suspects a security breach has occurred then immediately the network cable from the device should be removed and the machine shut down. DAT's administrative office should be informed straight away, or if no one is available in the office DAT's external IT contractor should be contacted.

Reporting

A brief cyber-security report detailing any breaches of security and other issues will be provided in DAT's quarterly reports.

Failure to comply

Failure to comply with this policy and procedures may result in disciplinary action.