



Information Security (InfoSec) Policy

Terminology:

Employee or member of staff: someone employed to work for the Business, whether as a fully employed person or as a contractor.

The Business: Web Design UK, or any of its other brand names.

1. Introduction

InfoSec is necessary to protect sensitive information and sensitive information systems from unauthorised access. Such as sensitive information use, disclosure, disruption, modification, or destruction.

The InfoSec function is also to provide confidentiality, integrity, and availability of sensitive information to those with authorised access.

2. Purpose

The process of protecting sensitive information assets of any format. It also applies to data in transit, processing or at rest in storage. This policy outlines the Business' processes.

3. Audience

All Web Design UK employees and Web Design UK clients that connect to any of our server systems. For example to use their email accounts.

4. Data Classification

See 'Data Classification & Access Policy' - <https://webdesignuk.agency/wp-content/uploads/2020/07/wduk-data-classification-and-access-policy.pdf>

webdesignuk

5. Access Control

See 'Data Classification & Access Policy' - <https://webdesignuk.agency/wp-content/uploads/2020/07/wduk-data-classification-and-access-policy.pdf>

6. Other Security, Access and Backup Measures

6.1 See Information Security Policy - <https://webdesignuk.agency/client-area/#our-policies>

6.2 Operating System & Browser Policy - <https://webdesignuk.agency/client-area/#our-policies>

6.3 Secure Password Policy - <https://webdesignuk.agency/client-area/#our-policies>

6.4 Service Level Agreement (SLA) - <https://webdesignuk.agency/client-area/#our-policies>

6.5 Mandatory Secure Erasure and Destruction Controls Policy - <https://webdesignuk.agency/wp-content/uploads/2020/07/wduk-mandatory-secure-erasure-and-destruction-controls-policy.pdf>

6.6 Change Management Policy - <https://webdesignuk.agency/wp-content/uploads/2020/07/wduk-change-management-policy.pdf>

6.7 Employment Policies - <https://webdesignuk.agency/client-area/contractor-forms/>

If you are unable to access any of the above policies owing to password protected pages, please open a support card to request access.

7. Training

All Web Design UK employees will take the online training course available here <https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available>

webdesignuk

The training must take place both during their induction, and every 12 months thereafter. Training scores will be recorded in their file.



Stay Safe Online Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand **why** you might be vulnerable to cyber attack, and **how** to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cyber security policies and practices that your organisation has already put in place.

Who is behind cyber attacks?

Online criminals

Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information for ransom.



Foreign governments

Generally interested in accessing really sensitive or valuable information that may give them a strategic or political advantage.

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.



Political activists

Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.

Terrorists

Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.



Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest mistakes

Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address.



© Crown Copyright 2018

Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a malicious website or an infected attachment.



Phishers use publicly available information about you to make their emails appear convincing. **Review your privacy settings, and think about what you post.**

Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.

Phishers often seek to exploit 'normal' business communications and processes. **Make sure you know your organisation's policies and processes to make it easier to spot unusual activity.**

Anybody might click on a phishing email at some point. **If you do, tell someone immediately to reduce the potential harm caused.**

Secure your devices

The smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks.



Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.

Always lock your device when you're not using it. Use a PIN, password, or fingerprint/face id. This will make it harder for an attacker to exploit a device if it is left unlocked, lost or stolen.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

Use strong passwords

Attackers will try the most common passwords (e.g. password1), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.



Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.

Use a separate password for your work account. If an online account gets compromised, you don't want the attacker to also know your work password.

If you write your passwords down, **store them securely away from your device. Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.**

Use two factor authentication (2FA) for important websites like banking and email. If you're given the option, 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

If in doubt, call it out

Reporting incidents promptly – usually to your IT team or line manager – can massively reduce the potential harm caused by cyber incidents.



Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.

Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.

www.ncsc.gov.uk [@ncsc](https://twitter.com/ncsc) [National Cyber Security Centre](https://www.facebook.com/nationalcybersecuritycentre)