Four Agency Worldwide

Policy: information security assurance

June 2024

This policy relates to Four Agency Worldwide (Four) and all its subsidiary companies including Four Communications, Four Marketing & Media, Four MSA (health media) and Four Communications Group FZ (MENA).

Background

This statement applies to those companies detailed in section 2 of FCG Worldwide Limited's External Privacy Notice and Workplace Privacy Notice, and the meaning of "Four" is defined in these notices. This statement is reviewed annually and approved by the board before issue.

Online

Four has voluntarily achieved Cyber Essentials Plus accreditation continuously since March 2015. This means that tests of Four's IT systems have been carried out by an external professional certifying body using a range of tools and techniques. Cyber Essentials Plus offers a higher level of assurance compared to the base level Cyber Essentials accreditation through the external and internal testing of the effectiveness of Four's policies and approach to IT security.

The most recent certification is valid until **1 May 2025**. A copy of the certificate is included with this statement, and a copy of the report provided by the certifying body is available upon request.

Cyber Essentials Plus accreditation concerns itself with five key controls of IT security:

1. **Boundary firewalls and internet gateways.**
   The good setup of these devices in hardware and/or software form is important for them to be fully effective. All endpoints are protected with endpoint-level web scanning technology to complement gateway systems. All internet-facing services undergo regular vulnerability scans.

2. **Secure configuration.**
   As well as designing and configuring all systems with security in mind (changing default passwords, turning off unneeded services, controlling configuration changes), passwords are set to expire routinely, to ensure regular password changes. No generic/shared accounts exist, and non-IT staff have no administrative-level credentials; all installations and configuration changes require such credentials.

3. **Access control.**
   Only those who should have access to systems have access and at the appropriate

level. Access to confidential and/or personal data is restricted to members of the relevant teams only, with senior managers personally verifying any changes. Staff have access only to those parts of Four's IT systems that they need to enter in order to carry out their normal duties.

Staff with Four email on their smartphone or tablet have additional security (including enforced 6+ digit codes with data encryption and remote wipe functionality). Remote access to Four's IT systems will shortly require the use of a two-factor system to prevent login credential abuse, to complement existing account lockout policies.

4. **Malware protection.**
   It is imperative to ensure that virus and malware protection is installed and kept up to date on all devices, regardless of the sensitivity of the data they access. This protection includes ransomware prevention systems, encryption guard/prevention, and zero-day signature-less behavioural monitoring of processes to prevent exploits. Multiple layers of ingress and egress protection ensure no threat vector is unmonitored. These systems provide real-time alerts to IT staff.

5. **Patch management.**
   The latest version(s) of applications are used, with a strict supported-only-versions policy; all necessary security and feature patches supplied by vendors are applied in a timely manner, typically under 14 days for security issues with a CVSS score >7. This patching includes plug-ins and freeware utilities as well as updates from key vendors such as Microsoft, Adobe, and Sophos.

In addition to these areas, Four takes further precautions to ensure the security, integrity, and availability of IT systems. These include:

6. **Backups, business continuity, and disaster recovery.**
   In the event of the failure of any one part of Four's IT systems, secondary copies of all data are held securely in environments that provide geographical, electrical, and connectivity resilience. These copies are replicated at least hourly, with pro-active monitoring and alerting setup. In many cases these replica copies can be made live within minutes.

   Remote access tools and portable devices (laptops, tablets, etc.) permit staff to work anywhere should any office become inaccessible. This is tested and reviewed regularly. Four has a full business continuity plan which includes how separate functions would operate in the event of different types of incidents; this is tested at least annually and all improvements reported and actioned within agreed timeframes. Evidence of this is available to clients and prospective clients upon request.

7. **Technical support and staff availability.**
   All IT systems are thoroughly documented and setup according to vendor and/or industry best practices, making support and administration straightforward. No

single person has sole access to any system, and a nominated third party provide reactive support services on a one hour SLA should it be necessary.

Helpdesk and monitoring tools identify where services are not performing as expected, allowing additional resources to be assigned proactively, and routine and reactive maintenance and health check efforts prevent technical issues from becoming services affecting.

8. **Logical organisation and policies.**
   Four voluntarily enforce a highly-structured and logical system for the storage of data, to prevent human error and make the security of systems easily manageable.

   Policies cover the use of all IT systems and these are covered as part of induction training for all staff joining the company, as well as policies covering the administration of Four's IT systems. These policies are reviewed regularly to ensure they provide relevant guidance to staff.

9. **Monitoring and proactive system integrity protection.**
   Four employs industry leading tools to monitor both the availability and integrity of all IT systems, as well as constantly checking activity and logs on these systems for risky or unusual processes, likely malicious activity, and indicators of compromise. This monitoring is linked to a 24x7 SOC (security operations centre) run by an ISO27001 and CREST certified organisation. They have SLAs that guarantee responses in under 15 minutes to all high risk alerts, initiating protective measures and full incident response processes where deemed necessary.

   Four also uses industry leading tools to frequently scan all IT systems on a frequent basis for possible issues that could affect the security, reliability, or availability of the services. This ensures all patching gaps can be remediated proactively, and the surface area for malicious attackers reduced to the smallest possible footprint.

Offline/physical security

1. **Operation of a "clear desk" policy and strict protocols on data retention.**
   In particular, no data is left unattended in the office if it could be considered confidential, personal, or otherwise covered under any contractual or legal obligations. All physical copies of data are securely disposed of when no longer required.

2. **All employees are issued with a unique access card or PIN to provide access.**
   Access cards act as both as a visual pass to enter the building, and as a "swipe card" to open doors locked using electronic access control and identify the user at printers, preventing print jobs being seen or taken by the wrong individuals. In other offices deemed lower-risk, PIN-based access control prevents opportunistic access to office areas. Separate PINs are used to identify users at printers.

3. **24x7 CCTV monitoring of all entry and exit points to our head office.**
   This gives full traceability in the event of a security incident, and sensitive areas

have out of hours proactive alerting should motion be detected. Other offices where risks are lower benefit from landlord CCTV covering entry and exit points to the premises.

4. **Security guards with SIA certification are on duty at all times at our head office.**
   They provide first line protection of access to our head office, and outside of normal business hours perform regular patrols throughout the building. These guards inspect the ID of all staff entering the building, with only senior staff permitted access without authorisation outside of normal business hours. Other offices have monitored alarm systems with multiple emergency contacts to alert staff to attempted unauthorised entry.

5. **Staff training.**
   All staff receive induction and routine training on how to handle data, and this is refreshed wherever the need is identified. Staff are also trained on other IT and non-IT systems; they are encouraged to report any concerns about IT, office, operational or client practices openly and promptly.

6. **Technical facilities.**
   Four uses only Tier 3+ data centre facilities, or cloud hosting partners operating to the same standard, to operate all IT systems. Depending on geography, these facilities hold ISO27001, SOC2 Type II, Cyber Essentials Plus, ISO23001, and other externally audited industry best practice standards to ensure the absolute security and availability of the systems hosted there. Access to these facilities is strictly limited to IT management.

four

CYBER ESSENTIALS PLUS

CERTIFICATE OF ASSURANCE

Four Agency Worldwide Ltd

The Hickman Building 2 Whitechapel Road London E1 1FX

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR : Jacob Ward

CERTIFICATE NUMBER : b1ff646a-146d-4ca8-b10e-23293b5bff25

PROFILE VERSION : 3.1 (Montpellier)

SCOPE : Whole Organisation

DATE OF CERTIFICATION : 2024-05-01

RECERTIFICATION DUE : 2025-05-01

SCAN QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK

CERTIFICATION BODY

CYBER ESSENTIALS PARTNER

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against a cyber attack.