netcraft
63 Catherine Place, London, SW1E 6DY, United Kingdom
+44 1225 447500 info@netcraft.com www.netcraft.com

Security Appendix

DOCUMENT CLASSIFICATION	Commercial in Confidence
DOCUMENT REFERENCE	SECCOMP-SEC-APP-1
VERSION	1.7
DATED	16th August 2024
OWNER	Security & Compliance
APPROVED BY	Matt Foster, Security Engineering Manager

1 Purpose

This Appendix describes Netcraft's security program, security certifications, and physical, technical, organisation and administrative controls and measures to protect customer data from unauthorised access, destruction, use, modification, or disclosure (the "Security Measures"). The Security Measures are intended to be in line with the commonly accepted standards of similarly situated software-as-a-service providers ("industry standard"). Netcraft will take reasonable steps to ensure its policies, procedures, and operations are set in accordance with Netcraft's obligations from this Appendix.

2 Updates and Modifications

The Security Measures are subject to technical progress and development; Netcraft may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially degrade or diminish the overall security of the cloud products, as described in this document.

3 Definitions

"Services" means the provision of the contractually agreed cloud services, products and/or data feeds by Netcraft to the Customer.

4 Security Measures

4.1 Security Management

Netcraft is certified by the UK Government's Cyber Essentials scheme with certificate number 3a2e1b73-e63c-4660-9e03-584694199cdc.

Netcraft has SOC 2 Type I compliance, please contact us to request a copy of the report.

4.2 Incident Handling and Response

Netcraft has a documented Incident Response (IR) plan to detect and react to security incidents, determine their scope and risk, and reduce the likelihood of similar incidents from reoccurring. Customer impact is assessed and if it is determined that there was any unauthorised use or loss of customer data, then the customer will be notified as soon as reasonably possible.

Netcraft has a documented Business Continuity and Disaster Recovery (BCDR) plan to minimise the impact of a realised risk event on the organisation.

Netcraft will periodically (no less frequently than annually) review, test, and, where applicable, update the BCDR and IR plans.

4.3 Access Control

Netcraft uses a custom single-sign on (SSO) system for customer authentication with a username and password. We support multi-factor authentication via time-based one-time password (TOTP). We support federated authentication using the SAML 2.0 protocol. Passwords are stored using a secure hash and salt algorithm.

Password policies are defined to ensure complex passwords for user accounts. Processes are in place to monitor employee access to shared user accounts; passwords to these accounts are rotated during internal role changes and staff offboarding.

Audit logs are maintained for both employees and customers, including login times, pages accessed, and actions taken.

An encrypted VPN is required for offsite access to internal systems. VPN access is protected by multi-factor authentication.

Netcraft grants the access rights of its engineers, testers, and technical operations team to the IT environments used for systems development according to the principle of least privilege.

Privileged access is reviewed at minimum once every 6 months and upon internal transfers.

4.4 IT Security

Netcraft's encryption tools leverage industry best practice, non-proprietary algorithms. Data encryption is mandatory for data-in-transit.

Our Services make use of TLS 1.2 or greater to encrypt data in transit over public networks. We also make use of TLS to secure communications where data is sent over the internet between our applications and databases. Our mail servers also support TLS, and we can configure mandatory TLS for transmission of emails if requested. Depending on the evaluated risk, data may be encrypted at rest while on our internal servers.

Netcraft utilises content delivery networks to mitigate the threat of a denial-of-service attack against key infrastructure.

Netcraft utilises a web application firewall to defend some internet-facing systems used in the provision and/or support of the Services.

Employee workstations have industry standard endpoint protection and anti-virus software installed. Detections are reported centrally and actioned promptly by the appropriate internal team.

Use of applications that may allow a user to bypass defined policies or escalate past granted privileges is restricted. Day-to-day employee workstation user accounts do not have local administrative privileges. Supplemental software is centrally curated and may be installed by users through a self-

service software portal. If required software is not available within this portal, subject to valid security and business requirements, a user may be issued ephemeral local admin credentials. These credentials may only be requested issued through a centralised, audited system, and only a limited set of staff are able to approve such requests.

4.5 Operational Security

Netcraft performs regular vulnerability scans on both internal and internet-visible infrastructure and remediates any issues in line with our vulnerability management policy.

Independent third-party penetration tests are conducted against our core services at least annually, and Netcraft has experienced internal pentesters who regularly test our customer facing and internal systems. Vulnerabilities discovered during testing are remediated in line with our vulnerability management policy, according to risk level. In addition, Netcraft uses AWS WAF and AWS Shield to protect our web applications from attacks.

Software patches are reviewed and deployed as dictated by the severity and service impact. Employee workstations and production servers regularly check for available updates and install them automatically when safe to do so. Otherwise, where an automated, unsupervised update has the possibility of causing downtime on a critical system, our systems administration team will be notified, and appropriate action taken. Results from our automated security scans additionally highlight out of date software and security patches and our systems administration and security teams monitor advisories and scans to ensure patches are installed. Server updates are handled via a centralised configuration management system, allowing automated control of system configurations, and resulting in consistent configuration changes and updates across the company.

Netcraft has a defined change management process. All approvals and changes are logged in our change management system.

Netcraft has documented backup policies and processes to ensure all essential information can be recovered. Backups utilise both tape-based and cloud-based solutions. Tape-based backups are stored at a separate office location and cloud-based backups are replicated across multiple availability zones. All backups are encrypted with AES-256. Backup procedures are regularly tested. Cloud based backups are also copied into a separate account, which has access limited to a very select group of trusted individuals.

Capacity management processes are in place, including 24x7 monitoring of Services and alerts sent to employees.

Netcraft maintains an inventory of hardware and software assets, with defined processes for acquisition and decommissioning. Reuse and reallocation processes are also in place. All removable assets are assigned to individual members of staff, with the assignment recorded.

4.6 Human Resource Security

Netcraft performs background screening on all relevant roles, including proof of right to work, criminal record check, and details of qualifications, experience, and previous employment.

All employees are required to agree to the company's policies and procedures, including relating to confidentiality, acceptable use, and ethics. Formal disciplinary processes are defined.

Netcraft has a defined entry and exit procedure for personnel changes that includes disabling user access rights upon termination of employment.

4.7 Physical Security

A physical access control policy is in place to prevent the unauthorised access, damage, and interference to Netcraft's premises and information:

i) All staff are issued with unmarked ID-cards/fobs for access, along with a separate identification card. Processes are in place for management of access for new hires and leavers.
ii) CCTV system in place at our primary office locations.
iii) Monitored alarm in place at our primary office locations, including entry / exit points and intrusion sensors.
iv) Visitor access polices are in place, restricted to organisation requirements and supervised unless previously approved.
v) A clear screen policy is in place. Automatic screen locks are configured via group policy.
vi) Laptop storage and portable drives are encrypted.

4.8 Data Storage and Retention

In general, Netcraft does not require personal or confidential data to provide our Services, except for employee names/email addresses for authentication and email alerts.

For some categories of countermeasures, such as social media impersonation or impersonation via email, letters of authorization containing images of ID may be required to prove Netcraft's ability to perform takedown requests on a customer's behalf. All such documents will be stored encrypted and only used as evidence when required.

Threat identifiers reported to Netcraft (for example, potentially malicious URLs, whether reported directly or extracted from a forwarded email) are not personal data and shall be owned by Netcraft. Threat identifiers may be shared with other organisations as part of the countermeasures process.

Our Services are hosted on Amazon Web Services (AWS) in Dublin, Ireland (eu-west-1) with London, UK (eu-west-2) utilised as a disaster recovery site. Some Services may also be hosted on DigitalOcean in London, UK, and Frankfurt, Germany and our self-hosted datacentre in Bath, UK. Further information can be provided upon request.

A data retention policy is defined individually for each aspect of the service and the internal processes feeding into it. This is based on evaluation of the requirements for retention and storage requirements. Records will be maintained for as long as they serve a business purpose, or which Netcraft has a legal, regulatory, or contractual duty to retain.

4.9 Vendor management

Netcraft has a vendor management policy which implements proportional, effective, risk-based controls for all third-party arrangements. Onboarding of third parties is subject to internal processes which assess and manage potential risk to compliance, reputation, and operations.

Netcraft is committed to acting ethically in all business dealings and expects all its suppliers to do the same. To this end, Netcraft maintains a Supplier Code of Conduct which articulates our commitment to ethical working conditions and business operations; and our expectations of our business partners.