NASSTAR

Security Policy

Level 1

POL003

NASSTAR

Contents

1 Purpose & Scope

This Security Policy is a customer-facing document, designed to provide the necessary assurance in relation to our security and data protection. It provides a guide to our commitment to security and what our customers can expect from us in this regard.

The Policy also details our approach to security and data protection in relation to the UK General Data Protection Regulations, and the Data Protection Act 2018.

It also outlines key recommendations for our customers in relation to security and data protection.

2 Introduction

We understand the importance of security and data protection and make every effort to ensure that customer information processed on our systems and other related areas are fully protected.

We recognise that the confidentiality, integrity and availability of information created, maintained, transmitted, stored and hosted by Nasstar and our customers is vital.

The management of Nasstar views this as one of its primary responsibilities, and fundamental to business best practice. We have therefore adopted and are certificated to the Information Security Management System (ISMS) Standard ISO27001:2013 through a UKAS accredited Certification Body. We are also certificated through the Cybers Essentials Scheme. We are adopting as best practice, ISO27701:2019 – "Extension to ISO/IEC27001 for Privacy Information Management".

The above allows us to manage and meet the following objectives which are to:

- Comply with all applicable laws, regulations and contractual obligations including the UK General Data Protection Regulation (UK GDPR), and the Data Protection Act 2018.
- Implement continual improvement initiatives, including risk assessment and treatment plans, while making the best use of our management resources to meet and improve information security management system requirements.
- Communicate our security and data protection objectives and our performance in achieving these objectives, throughout the Company and to interested parties.
- Maintain a Policy, Code of Conduct and Standard Operating Procedures that provide direction and guidance on security and data protection matters relating to employees, customers, suppliers and interested parties who come into contact with our activities.
- Work closely with customers, business partners and suppliers in seeking to establish appropriate standards.
- Adopt a forward-looking view on business decisions, including the continual review of risks which may have an impact on security and data protection
- Constantly strive to meet, and when possible exceed, customer and employee expectations.
- Consider security and data protection in role guides and when setting employee objectives where applicable.
- Provide security and data protection training and awareness to all employees to ensure responsibilities, principles and practices are embedded in our culture.

3 Nasstar's Security Governance & Certification Framework

- Nasstar is ISO 27001:2013 certificated by United Registrar of Systems (URS);
- We also hold the Cyber Essentials Certification.
- The senior management team has overall responsibility for security within Nasstar which is delegated from the Board who retain accountability.

- We are also adopting as best practice, the requirements of ISO27701:2019 – "Extension to ISO/IEC27001 for Privacy Information Management" which integrates with our ISMS and overall Business Management System.
- An Internal Audit Programme is in place as part of our ISO27001 certification
- A Global Information Security, Data Protection and Privacy Policy, supported by a Code of Conduct and suite of standard operating procedures, is in place, including a risk-based methodology incorporating Data Protection Impact Assessments and treatment plans which run across all operational aspects of the business.
- Our Documents, Records and Information Management Standard Operating Procedure addresses retention periods amongst other things.
- Nasstar is also certified to PCI DSS v3.2.1, ISO 9001:2015, ISO20000-1:2018, ISO 14001:2015 and adopts the principles of ITIL.

4 Nasstar Security – Key Elements

4.1 Physical Security

- All Nasstar locations incorporate industry standard security controls, covering physical perimeter, CCTV and monitoring along with logged card access systems.
- These controls are underpinned and supported by our ISO27001:2013 certification.
- Unaccompanied access to data centre facilities is not permitted and is detailed in our Physical Security Standard Operating Procedure and our Access Control Standard Operating Procedure.

4.2 Operational Security

- We adopt a Configuration and Change Management process, in line with ISO27001, PCI DSS and ITIL. A dedicated Change Manager oversees all potential security-impacting changes to service. These are tracked and recorded to completion of the change.
- We have adopted an ISO27001 and PCI DSS compliant vulnerability management strategy. As well as targeted penetration testing, our team of engineers stay up-to-date with the latest threats and exploitation techniques being used. Any threats that warrant action are tracked through Change Management until completion.
- A SIEM (Security Information and Event Management) solution utilising FortiSIEM is utilised to provide real-time analysis across the core infrastructure of events and security alerts generated by applications, network and security hardware.
- Corporate infrastructure has an End Point Protection solution that detects, prevents and responds effectively to known malware, threats of traditional anti-virus and zero day exploits.
- Vulnerability scanning is performed regularly across the infrastructure for the detection of potential points of exploitation and security holes and checked against publicly disclosed vulnerabilities known as Common Vulnerabilities and Exposures (CVE).
- Incident Management is an integral part of our security procedures based upon ISO 27001:2013 and ITIL. Security Incident Response Teams are used to manage incidents effectively.
- Customers consume services in the form of IaaS, SaaS, PaaS and CSaas (Cyber Security as a Service). All underlaying technology for supporting / maintaining these platforms is restricted to authorised employees only.

4.3 Supply Chain Management

- We utilise Data Centres and communication infrastructure supplied and or managed by 3rd parties, details can be provided on application. None of these 3rd parties have logical access to information or management system. ISO27001 certification is still required for these sites.

- We ensure supplier selection and approval criteria, security and data protections requirements, and performance monitoring are utilised which are proportionate to the risk and the information processed.

4.4 Secure Development & Deployment

- We design all dedicated implementations in-line with current industry practice and employ a Secure Development Policy in-line with ISO 27001:2013. Throughout development, testing and deployment we are responsible for all software security updates on our platforms in conjunction with supplier and manufacturers. For customers with dedicated solutions, engineers manage the availability and control of security updates released to customers via approved deployment tools or processes.
- CREST certified PEN Tests and vulnerability scans are conducted as required by our certifications at least annually to capture new and evolving threats. Resulting actions are risk assessed, prioritised and treated in line with our ISO27001 and PCI DSS Risk Management requirements and overseen by the Governance, Standards and Assurance Team.

4.5 Access Control

- Access to our internal systems, hosting platform and customer servers is permitted for authorised personnel only. All users must be positively identified by providing a secure User ID and password before being given access to system resources. Incoming callers are identified using details taken from their accounts. Additional password protection can be applied for sensitive environments.
- All servers, routers, firewalls and network equipment are protected by multi-factor authentication technologies or with a minimum of a password. All passwords are randomly generated for optimum security to prevent intruders gaining unauthorised access to systems and information.
- Only 3rd Line Engineers have full access to hosted platforms, each engineer having their own individual login for optimum security. Authorised support staff have Admin access to hosted services in order to provide technical support to customers.
- Where Support Engineers require access to our network and systems and are external to our Corporate infrastructure, they will connect via VPN technologies. Two factor authentication technologies are used to encrypt and secure the communications.
- Solutions are accessed either via VPN or via client-side licensed software (such as Skype for Business and Teams), both requiring authentication.
- Accessing the internet-facing Support Portal also requires authentication and complex passwords with lockout and reset rules. The support portal gives access to customer contact information and our SLAs, but not access to the Cloud environment itself.

4.6 Employee Screening

- We perform the necessary background employment checks commensurate with the sensitivity, criticality, and potential liability for the job function and service which we are offering. All employees involved in technical service provision are vetted to the Baseline Personnel Security Standard Plus, or the equivalent standards for our overseas operations.
- All employees are given Information Security training as part of their induction and a minimum of every 12 months thereafter, in support of our ISO 27001:2013 certification.

5 Recommendations for Customers

The purpose of these recommendations is to help prevent unauthorised access to our Services, including to help ensure the security of our own network and infrastructure where this could be impacted by a breach of security in the Customer's own network or infrastructure, or unauthorised access to the

Services or administrative controls granted to the Customer in respect of these, including Customer portals.

5.1 Passwords

Network and other devices (including but not limited to firewalls) should be securely configured on installation, and the default administrative password for any network and other devices should be changed to an alternative, strong password, as default passwords are often publicly known.

A strong password is typically one that:

- comprises a minimum number of characters in length (e.g., 8 characters).
- differs from the associated username.
- contains no more than two identical characters in a row.
- is not a dictionary word.
- includes a mixture of numeric and alpha characters.
- has not been reused within a predetermined period of time (e.g., 6 months); and
- has not been used for another account.

Similarly, any default password for a user account should be changed to an alternative, strong password, and administrative user accounts should be configured to require a password change on a regular basis (e.g. at least every 90 days).

5.2 User Access Control

User accounts, particularly those with special access privileges (e.g., administrative accounts) should be assigned only to authorised individuals, managed effectively, and provide the minimum level of access to applications, computers and networks.

Special access privileges should be restricted to a limited number of authorised individuals and reviewed regularly.

The use of shared accounts should be avoided due to the impact these can have on auditing and post incident investigations.

User accounts and special access privileges should be removed or disabled when no longer required (e.g., when an individual changes role or leaves the organisation) or after a pre-defined period of inactivity (e.g., 3 months).

5.3 Anti-virus, Malware & Patching

Ensure up to date Antivirus and Malware is installed on all relevant systems and devices. This will provide a basic level of protection against malicious software being installed on systems which may can steal sensitive information such as account credentials or banking details. Consider prioritising patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months.

5.4 Physical Security

Ensure all communications equipment is kept secure from unauthorised access to avoid the risk of tampering. If equipment must be located in areas without access restrictions, consider the use of a lockable 'comms cabinet' to house it.

5.5 Further Guidance

The foregoing recommendations are only a small number of security measures which a Customer should consider adopting to help defend itself against cyber threats and represents guidance only. They do not represent all of the security controls an organisation needs to have in place to protect against such threats.

Useful further information is contained in the Government's Cyber Essentials Scheme which sets out requirements for basic technical protection from cyber-attacks.

6 Document Control

Any suggested changes or amendments must be communicated through the author for consideration and inclusion if suitable.

Version	V5.0
Release Date	10/03/2021