Acceptable Use Policy (AUP)

IT & Security

Class 1 – General B2B Use / Public

Version 2.0 - 07/05/2026

Contents

1 Purpose & Objectives 3
2 Scope 3
2.1 Compliance Obligations 4
3 Breach Management, Exceptions & Escalations 4
4 Policy Statement 4
4.1 AUP Principals 4
4.2 What You Must Do 5
4.3 What You *Must Not* Do 5
4.4 Monitoring & Privacy 5
5 Roles and Responsibilities 6
6 Policy Governance 7
7 Definitions & Acronyms 7

Version Control

Current Version

Parameter	Value
Current Version	2.0
Release Date	07/05/2026
Author	Dan Kennoy, Chief Information Security Officer

Version History

Version	Date	Author	Description of Changes
DRAFT	06/06/23	GMT	First draft of new AUP.
1.0	01/08/23	GMT	New AUP introduced following internal review and approval.
1.1	10/01/2024	GMT	Minor amendments made to language and terminology used. No new content added to this policy.
1.2	28/05/2025	Dan Kennoy, Chief Information Security Officer	Minor amendments and the addition of statement around copyright licences relating to streaming.
2.0	07/05/2026	Shannon Huxley, Head of Risk & Compliance	Changed document type to a policy, updated format. Added use of AI principles.

1 Purpose & Objectives

This policy defines the minimum acceptable requirements for the use of Nasstar information assets to protect the confidentiality, integrity, and availability of information and systems.

The objectives of this policy are to:

- Ensure information assets are used appropriately and securely.
- Reduce the risk of data loss, security incidents, and legal or regulatory breaches.
- Protect Nasstar's reputation, intellectual property, and customer information.
- Support compliance with information security, data protection, and contractual obligations.

This policy supports Nasstar's Integrated Management System (IMS) and Information Security Management System (ISMS).

2 Scope

This policy applies to:

- All Nasstar Group companies and operating divisions

- All employees, contractors, temporary workers, agency staff, and third parties acting on Nasstar's behalf
- All Nasstar information assets, including systems, networks, applications, devices, data, and cloud services.
- All locations and working environments, including remote and mobile working.
- There are no exclusions to this policy.

2.1 Compliance Obligations

This policy supports compliance with:

- ISO/IEC 27001:2022
- Applicable data protection and cyber security legislation
- Contractual and customer security requirements
- Nasstar internal policies, standards, and codes of conduct

3 Breach Management, Exceptions & Escalations

Breach Reporting

Any suspected or actual breach of this policy must be reported promptly via:

- Line management
- The IT and Security function
- Email: **Compliance@nasstar.com**
- The Whistleblowing process, where appropriate

Exceptions

Exceptions to this policy are permitted only where there is a legitimate business requirement and must:

- Be formally requested. Please submit this request via email to compliance@nasstar.com detailing the rationale for the requested exception.
- Be approved in writing by the appropriate authority including the CISO
- Be time-limited and documented

4 Policy Statement

4.1 AUP Principals

- Use Nasstar systems and equipment for authorised business purposes only.
- Protect information from unauthorised access, disclosure, alteration, or loss.
- Comply with all security controls, including authentication and access controls.
- Prevent unauthorised software, hardware, or services from being connected to Nasstar systems.
- Ensure Nasstar data is not stored, processed, or transmitted using unauthorised personal devices, email accounts, or cloud services.
- Reboot or update devices when prompted to ensure security patches are applied.
- Protect Nasstar's reputation by using internet and social media responsibly.

- Avoid accessing, creating, storing, or transmitting inappropriate, illegal, offensive, or discriminatory material using Nasstar systems.
- Respect copyright, licensing, and intellectual property obligations

4.2 What You Must Do

- ✓ Use Nasstar systems, devices, and accounts for authorised business use.
- ✓ Protect usernames, passwords, MFA tokens, and access credentials.
- ✓ Lock your screen and secure devices when unattended.
- ✓ Follow security prompts (updates, reboots, password changes).
- ✓ Store and share information only using approved Nasstar systems.
- ✓ Report security incidents, mistakes, or concerns immediately.
- ✓ Use the internet, email, and collaboration tools responsibly and professionally.

4.3 What You *Must Not* Do

- ❌ Use personal email, cloud storage, or messaging apps for Nasstar data.
- ❌ Install unauthorised software or connect unauthorised devices.
- ❌ Circumvent security controls or monitoring.
- ❌ Access, create, store, or share illegal, offensive, or inappropriate content.
- ❌ Use Nasstar systems for activities that could damage Nasstar's reputation.
- ❌ Share confidential or customer information without authorisation.

4.4 Monitoring & Privacy

Nasstar systems, networks, and devices may be monitored, logged, and reviewed to:

- Maintain security and performance.
- Detect unauthorised or malicious activity.
- Support investigations and regulatory compliance.
- Monitoring is conducted lawfully and proportionately in line with applicable privacy and employment legislation.

4.5 Acceptable Use of Artificial Intelligence (AI)

Users of AI tools must:

- Use only approved AI tools for legitimate business purposes.
- Not input confidential, restricted, personal, or customer data into public or unapproved AI systems.
- Treat AI outputs as unverified and review before use in any business or customer context.
- Ensure AI use does not breach legal, contractual, or intellectual property obligations.
- Not use AI to create or distribute misleading, harmful, or inappropriate content.

5 Roles and Responsibilities

Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is accountable for the overall direction, governance, and effectiveness of information security across Nasstar. The CISO is responsible for:

- Owning and approving the Acceptable Use Policy and associated information security standards.
- Overseeing the implementation and operation of appropriate technical and organisational controls to support acceptable use.
- Acting as the escalation point for significant or high-risk breaches of this policy, including major security incidents.

Risk & Compliance

The Risk & Compliance function is responsible for oversight, assurance, and alignment of the Acceptable Use Policy with Nasstar's governance and compliance framework. This includes responsibility for:

- Ensuring acceptable use requirements align with Nasstar's risk appetite, regulatory obligations, and ISO 27001 requirements.
- Providing senior management with assurance on compliance, incidents, trends, and emerging risks related to acceptable use.
- Supporting monitoring, reporting, and management review activities relating to policy compliance.

First Line – Doing the work	Second Line – Setting the rules and checking	Third Line – Independent assurance
Managers & Users • Ensure day-to-day compliance with this policy. • Protect access credentials and information assets. • Report incidents or weaknesses promptly. **IT & Security:** **Examples:** • System logging • SIEM monitoring • Endpoint detection • DLP alerts • Access control enforcement • Automated compliance evidence collection	**Risk & Compliance** • Define acceptable use requirements. • Monitor compliance and provide guidance. • Review and maintain this policy. **IT & Security:** **Examples:** • Reviewing logs and alert trends • Monitoring compliance dashboards • Assessing whether controls meet policy and risk appetite • Challenging control effectiveness	**Internal Audit:** • Independently assess whether controls exist. • Evaluate whether they are designed appropriately. • Test whether they are operating effectively. • Confirm segregation between first and second line.

6 Policy Governance

This policy is to be reviewed on a minimum of an annual basis or in line with business or regulatory landscape changes.

All stakeholders under the scope of this policy are obligated to promptly report any breaches by emailing Compliance@nasstar.com

Definition of non-adherence includes, but is not limited to:

- Failure to follow any stated rule, procedure, or protocol outlined within this policy.
- Deliberate circumvention of control measures, processes, or systems established to support this policy.
- Negligent actions or omissions that result in a breach or violation of the policy's intent or requirements.

Any confirmed instance of non-adherence to this policy, regardless of whether it results in immediate loss or harm to the Company, will be treated as a serious matter of misconduct and may result in the trigger of the Nasstar's formal Disciplinary Procedure.

7 Definitions & Acronyms

- **AUP** – Acceptable Use Policy
- **IMS** – Integrated Management System
- **ISMS** – Information Security Management System
- **Information Asset** – Any data, system, device, or service used to store, process, or transmit information