Technical Policy - Information Security

1. Purpose, Scope and Users

Highwire Inc., (Highwire), maintains a strong security program that includes policies, procedures, plans, and controls that protect the company's information assets, including but not limited to information technology (IT) systems, the Highwire application, and sensitive data. The purpose of this policy is to provide a high-level understanding of the principles and practice of Highwire's Information Security Management System (ISMS).

The scope of this policy applies to the entire Information Security Management System, as defined in the Highwire ISMS Scope document.

Users of this policy are all employees of Highwire, as well as any relevant external parties.

2. Reference Documents

This document was developed as the central information security policy for Highwire. While this policy provides the general approach to information security, it is supplemented by very specific administrative and technical policies including those listed below. This and other policies, manuals and reports associated with our ISMS are available for internal viewing on the Highwire Compliance Shared Drive in Google Workspace. Clients and Contractors of Highwire can request a copy of specific technical policy(ies) by contacting support@highwire.com.

- Highwire Acceptable Use Policy
- Highwire Access Control Policy
- Highwire Change Management and Secure Development/Engineering Policy
- Highwire Clear Desk and Clear Screen Policy
- Highwire Data Backup Policy
- Highwire Data Quality Assurance & Quality Control Policy
- Highwire Document & Information Control Policy
- Highwire Encryption Policy
- Highwire Incident Management Policy
- Highwire Internal & External Audit Policy
- Highwire Logging and Monitoring Policy
- Highwire Password Policy

- Highwire Privacy Policy

In addition to the above policies, the following internal documents have also been prepared in accordance with the ISO/IEC 27001:2022 Standard; System & Organization Controls (SOC), published by the American Institute of Certified Public Accountants (AICPA); the European Union General Data Protection Regulation (GDPR), 2018; the EU-U.S. & Swiss-U.S. Data Privacy Frameworks, the UK Extension to the EU-U.S. Data Privacy Framework, and the California Consumer Privacy Act (CCPA). These documents are also considered reference material to this over-arching Information Security Policy:

- Highwire ISMS Statement of Applicability
- Highwire ISMS Scope Document
- Highwire ISMS Risk Assessment and Risk Treatment Methodology
- Highwire ISMS Risk Assessment and Risk Treatment Report

Finally, there are several internal Highwire manuals that contain information that is relevant to our information security and how we communicate that to employees and clients, including:

- Highwire Asset Management Manual
- Highwire Communications Manual
- Highwire Contract Management Manual
- Highwire Customer Support Manual
- Highwire Disaster Recovery and Business Continuity Manual
- Highwire Employee Handbook
- Highwire Employee Training and Development Manual
- Highwire Governance Manual
- Highwire Human Resources Manual
- Highwire Regulatory Review Manual
- Highwire System Architecture Manual
- Highwire System Hardening Manual
- Highwire Vendor Management Manual
- Highwire Workplace Safety Manual

3. Information Security Objectives

The three guiding objectives of Highwire's information security are confidentiality, integrity, and availability:

Confidentiality: The goal of confidentiality is to ensure that information is only available to authorized persons or systems. Confidentiality is critical to total data security. In general, the controls that we have in place regarding confidentiality include encryption, virtual private network connections, employee vetting and strict non-disclosure requirements, and many others. Specific controls are fully detailed in the various ISMS supporting documents as listed above in Section 2.

Integrity: The goal of integrity is to ensure that information is only allowed to be changed by authorized persons or systems in an allowed way. This objective includes both data integrity and system integrity. In general, the controls we have in place to protect the integrity of our data and our system include access control, firewalls, encryption, logging and monitoring, and many others. Specific controls are fully detailed in the various ISMS supporting documents as listed above in Section 2.

Availability: The goal of availability is to ensure that information can be accessed by authorized persons when it is needed. In general, the controls that we have in place regarding availability include authentication, authorization, password control, and many others. Specific controls are fully detailed in the various ISMS supporting documents as listed above in Section 2.

To achieve our guiding objectives, Highwire relies on an overall Information Security Management System that allows for planning, implementing, maintaining, reviewing, and improving information security. While the ideals behind our guiding principles may seem too general to measure, Highwire utilizes the S.M.A.R.T. concept to establish demonstrable ways to determine our success in achieving the confidentiality, integrity, and availability of our system. We have developed a checklist of items that are Specific, Measurable, Achievable, Relevant, and Time-based. This checklist is reviewed at least annually by the Vice President of Engineering and the Vice President of Compliance and the results are tracked, analyzed, and included as part of the ISMS Management Review meeting(s). The checklist is included as Appendix 1 to this policy.

4. Roles and Responsibilities

Highwire has defined 4 principal roles for the development, maintenance and continuous improvement of our Information Security Management System. These roles are held by the Senior Vice President of Finance, the Vice President of Engineering, the Director of Engineering, and the Vice President of Compliance. Together these 4 positions make up the Information Security Management System Committee. In general, the roles are defined as:

Sr. Vice President, Finance	• Ensure that the ISMS satisfies the requirements of ISO27001 and Type I SOC 2 controls. • Ensure that Highwire's hiring process is followed for all prospective employees, including the completion of background checks. • Chair the annual ISMS Management Review Meeting, including the Vice President of Engineering and the Vice President of Compliance, to review the suitability, adequacy, and effectiveness of the ISMS. • Ensure that the ISMS is a critical priority for the entire organization and is addressed adequately in both employee onboarding training and annual training. • Ensure that the appropriate resources are available to support the development, maintenance, and continuous improvement of the ISMS.
Vice President of Engineering	• Act as the Chief Information Security Officer (CISO) as defined in ISO27001. (Note that the terms CISO and Vice President of Engineering are considered interchangeable throughout our company and ISMS documentation). • Act as the Technical Project Manager as defined in the ISMS Project Plan. • Develop, maintain, review and enforce all technical ISMS documents and policies as listed in the ISMS Project Plan and ISMS Scope. Specifically, this is accomplished by completing the ISMS Comprehensive Compliance Measurement Review table that is detailed in the Highwire Information Security Policy. • Manage all incidents, including any corrective actions, and track, analyze, and report incidents to the CEO.

Director, Engineering	• Coordinate with the VP of Engineering for the development and maintenance of all Highwire architecture, networks, software and systems. • Responsible for all server infrastructure including all security architecture and AWS infrastructure. • Responsible for development protocols and standardization, including code conformance and review. • Responsible for secure and efficient deployment structure and processes.
Vice President of Compliance	• Act as the Administrative Project Manager as defined in the ISMS Project Plan. • Develop, maintain and review all Highwire manuals (e.g., Highwire Human Resources Manual, Highwire Administrative Manual, Highwire Customer Support Manual, Highwire Vendor Management Manual, Highwire Disaster Recovery and Business Continuity Manual). • Perform an evaluation of current regulations, and review any new regulations as they arise, to determine applicability. • Develop/Conduct annual and onboarding training for Highwire employees on company policies and the ISMS and ensure that access is provided to all company manuals, policies, and ISMS documentation. Annual training slides can be found in the Highwire shared Google drive. • Maintain an inventory of company assets. • Take and maintain minutes from all critical ISMS meetings.

Highwire has also identified 4 other internal roles that, while they don't sit on the ISMS Committee, they do provide important support to the ISMS:

Sr DevOps Engineer	• Perform quarterly access review for approval by Director, Engineering. • Deliver necessary updates to SSL Policies on ALB, EKS, New Relic, and PostGres. • Conduct internal auditing as necessary.

Director, Talent Operations	• Manage the Gusto Human Resources platform. • Manage employee onboarding and offboarding. • Complete annual update of the Highwire Employee Handbook and deliver via Gusto for annual signature by all employees. • Manage the LearnUpon Training platform that powers Highwire University. • Ensure that the appropriate HR resources are available to support the development, maintenance, and continuous improvement of the ISMS.
Vice President, Marketing	• Develop and deliver the monthly Client email with new functionality releases. • Develop and deliver Contractor communications to announce key functionality updates. • Manage the Highwire website, including updates to the Terms, Privacy Policy, and blog entries regarding data security.
Sr. Manager, Finance	• Manage Client billing. • Manage Contractor billing and review refund requests • Manage the Stripe credit card integration. • Manage fraud investigations in Stripe.

In addition to the above general roles, Highwire has developed a RACI table to specify responsibilities under the ISMS. The table defines who is **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed, and who is a **Q**uality Reviewer. As is typical with the RACI concept, the Responsible party is defined as the person(s) who completes the task and the Accountable party is defined as the person who is ultimately answerable for the activity or decision. There can be more than one person identified as Responsible, Consulted, Informed, or Quality Reviewer. However, only one person can be named as Accountable.

	ISMS Governance Committee				ISMS Support Team			
	SrVP, Fin	VP, Engg	Dir, Engg	VP, Comp	Dir, Talent	VP, Market	SrMgr, Finance	Sr. DevOps
Review of Information Security Policy	A	R	R	Q	I	I	I	Q
Communicate Information Security Policy to staff	A	I	I	R	Q	R	I	I
Communicate Information Security Policy to 3rd parties	A	I	I	R	I	R	I	I
Review of Acceptable Use Policy	A	R	R	Q	Q	I	I	Q
Review of Change Mgmt/Secure Engg	A	R	R	Q	I	I	I	Q
Review of Clear Desk Policy	A	R	R	Q	Q	I	I	Q
Review of Data Backup Policy	A	R	R	Q	I	I	I	Q
Review of Data Quality Assurance and Quality Control Policy	A	R	R	Q	I	I	I	Q
Review of Document and Information Control Policy	A	I	I	R	Q	I	I	I
Review of Encryption Policy	A	R	R	Q	I	I	I	Q
Review of Incident Management Policy	A	R	R	R	Q	I	I	Q
Review of Internal Audit Policy	A	R	R	Q	I	I	Q	Q
Review of Logging & Monitoring Policy	A	R	R	Q	I	I	I	Q
Review of Password Policy	A	R	R	Q	I	I	I	Q
Review/Update of Risk Assessment	I	A	I	R	Q	I	I	Q
Review of Governance and Related Admin Manuals	A	C	C	R	Q	I	I	Q

Conduct Legal and Regulatory Review	A	C	I	R	Q	I	Q	I
Update Asset Inventory	A	I	I	R	Q	I	Q	I
Review of Employee Handbook	A	C	I	Q	R	I	I	I
Review of Customer Support Manual	A	C	I	R	I	Q	I	I
Review of Contracts	A	C	I	R	I	I	Q	I
Review & Test of Disaster Recovery Manual	I	A	R	R	I	I	I	R
Review of System Architecture Manual	I	A	R	Q	I	I	I	Q
Review of System Hardening Manual	I	A	R	Q	I	I	I	R
Conduct Internal Audit	A	C	R	R	I	I	R	R
Conduct Measurement of ISMS Objectives	A	R	R	R	I	I	I	R
Conduct Pen Testing	I	A	R	R	I	I	I	Q
Conduct DCI PSS Audit	I	A	R	R	I	I	I	I
Conduct HR and ISMS Training	A	I	C	R	R	I	I	I
Manage Facility Issues	A, C	I	I	R	R	I	R	I

5. Managing Information Security

This policy, and all referenced documents, outline Highwire's Information Security Management System (ISMS) in order to protect the organization's information assets against all threats, whether internal or external, deliberate or accidental. Highwire relies on the highest standards of practice to meet our security challenges, including those requirements published by the International Organization for Standardization (ISO) as part of ISO/IEC 27001:2022; the American Institute of Certified Public Accountants (AICPA) as part of their System & Organization Controls (SOC); the European Union as part of the General Data Protection Regulation (GDPR); the California Consumer Privacy Act (CCPA); the Payment Card Industry Data Security Standard (PCI DSS); and, best industry practices. This Information Security Policy ensures that the principles of confidentiality, integrity, and availability will be met.

Specific tenets of this Information Security Policy include:

a. Buy-in for the planning and implementation of the ISMS is at the highest level of the organization. Specifically, the Chief Executive Officer and the Senior Vice President of Finance have approved all aspects of the ISMS, including but not limited to this policy and is committed to ensuring that the necessary resources are available to support the ISMS. The Senior Vice President of Finance is responsible for staff compliance across the organization.
b. The Information Security Policy ensures that there is clear responsibility for the development and review of information security objectives. Specifically, all technical policies are developed through the joint efforts of members of the Highwire Engineering Department and are reviewed and published at least annually by the Vice President of Engineering. The Vice President of Engineering is designated as the Information Security Manager as defined by ISO/IEC 27001:2022. All administrative and human resource policies are developed by the Vice President of Compliance and the Director of Talent Operations and are reviewed at least annually by the Senior Vice President of Finance.
c. The Information Security Policy ensures that both the Director of Engineering and the Vice President of Compliance formally report to the Senior Vice President of Finance the performance of their relevant areas of the ISMS at least three times per year, but due to the small size of the organization and the open working environment, conversations about maintaining, improving, and exceeding the requirements of the ISMS are a continual process and are integrated into Highwire's day-to-day business.
d. The Information Security Policy ensures that the ISMS is compliant with relevant legal and regulatory requirements and contractual obligations as detailed in the Highwire Regulatory Review Manual.
e. The information Security Policy ensures that the ISMS clearly defines control over the creation, classification, approval, distribution, storage, and usage of updates of documents, records, information, and data used by Highwire as detailed in the Highwire Document and Information Control Policy.
f. The process of selecting appropriate controls and measures to safeguard our information assets is defined in the Highwire ISMS Risk Assessment and Risk Treatment Methodology and is reviewed continuously by the Director of Engineering to ensure that the ISMS is robust and evolves as new security technologies develop.
g. The process of auditing and measuring the effectiveness of our selected controls is conducted as outlined in various ISMS documents, including the Highwire Internal & External Audit Policy, and with Section 6 below.

h. Business continuity plans will be developed, maintained, and tested as defined in the Highwire Business Continuity Manual.
i. Training and awareness with this policy, and other referenced ISMS documents, is conducted as part of Highwire's overall employee training program as detailed in the Highwire Employee Training and Development Manual. As part of the training, employees are informed about the ISMS, provided with access to reference documents, and must sign off on acknowledgement and agreement with the overall ISMS and, specifically, this policy. In addition, an annual company-wide meeting is held where the ISMS is reviewed to ensure ongoing suitability, adequacy, and effectiveness. Detailed minutes of that annual meeting are prepared and maintained by the VP of Compliance.
j. All actual or suspected security breaches will be reported to the Vice President of Engineering and will be thoroughly investigated as defined in the Highwire Incident Management Policy and the Highwire Disaster Recovery and Business Continuity Manual. Notification of personal data breaches or fraud will be reported to affected users as required by the GDPR, the EU-U.S. & Swiss-U.S. Data Privacy Frameworks, the UK Extension to the EU-U.S. Data Privacy Framework, and as defined in the Highwire Privacy Policy.
k. All employees, including the Chief Executive Officer, the Senior Vice President of Finance, the Vice President of Engineering, the Director of Engineering, and the Vice President of Compliance are committed to continual improvement of the ISMS and work closely with clients to establish the highest quality standards and to ensure that they are partners in our commitment to information security.

6. Measuring the Effectiveness of Information Security Controls

a. Compliance Criteria

When evaluating the effectiveness and adequacy of this particular policy, the following criteria must be considered:

- Number of employees who have a role in the ISMS, but are not familiar with the Highwire Information Security Policy and know where to access it online;
- Percent of clients and external parties who have been communicated with on the Highwire Information Security Policy and who have been provided a copy on annual basis (and whenever there is a new version); and,
- Number of reviews of laws and regulations for applicability to Highwire operations in a 12-month period.

b. Compliance Measurement

The specific compliance criteria bulleted above are included as part of an ISMS Comprehensive Compliance Measurement Table that has been prepared by Highwire and is provided in Appendix 1. The Vice President of Engineering and the Vice President of Compliance will verify compliance with our overall Information Security Policy, and all other technical policies, by performing a review, at least annually, using the ISMS Comprehensive Compliance Measurement Table. The results of the annual review will be tracked, analyzed, and included as part of the ISMS Management Review meeting(s).

In addition to the formal annual review, compliance is also measured on a continual basis through various methods, including but not limited to, periodic walk-throughs, business tool reports, and feedback to the policy owner.

c. Exceptions

Any exception to the policy must be approved by the policy owner in advance.

d. Non-Compliance

An employee found to have willfully violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. Review and Development

The author of this policy is considered the policy owner and is responsible for updating it whenever changes are dictated by the work. In addition, a quarterly review of the Information Security Policy will be conducted by the Vice President of Engineering to ensure that this overarching technical policy remains appropriate considering any relevant changes to the law, organizational policies, and/or contractual obligations. Any revisions to this policy resulting from any quarterly review will be noted in the Versioning Table below.

As specified in the Highwire Document and Information Control Policy, all changes to an ISMS document must be made using “track changes”, making visible only the revisions to the previous version, either showing them in red text or strikeout. In addition, for reference, all previous versions of an ISMS document are stored on the personal user drive of the Highwire Vice President of Compliance. The versioning history is defined in the table below:

Version History	Date	Author	Approver	Classification
Version 9	5/14/24	K. Sardone	H. Bhinder	Public

Version 8	6/1/23	K. Sardone	N. McIntyre	Confidential
Version 7	5/16/22	S. Kirilenko	N. McIntyre K. Sardone	Confidential
Version 6	2/17/22	S. Kirilenko	N. McIntyre K. Sardone	Confidential
Version 5	4/1/21	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
Version 4	1/21/20	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
Version 3	5/15/19	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
Version 2	7/3/18	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
Version 1	10/24/17	S. Kirilenko	D. Milinazzo, K. Sardone	Confidential
This policy will be reviewed quarterly and updated at least annually by the Vice President of Engineering.				

8. Appendices

Appendix 1 – ISMS Comprehensive Compliance Measurement Table.

Objective	Measurement	Target	Document Reference	Responsibility
Integrity	Number of employees who have a role in the ISMS, but are not familiar with the Highwire Information Security Policy and know where to access it online.	0	Information Security Policy	K. Sardone
Integrity	Percent of clients and external parties who have been communicated with on the Highwire Information Security Policy and who have been provided a copy on an annual basis (or whenever changed).	100%	Information Security Policy	K. Sardone

Confidentiality Integrity Availability	Number of reviews of laws and regulations for applicability to Highwire operations in a 6-month period.	1	Highwire Regulatory Review Manual	K. Sardone
Confidentiality Integrity	Number of incidents related to unacceptable use of information assets, including instances of asset loss or compromise.	0	Acceptable Use Policy	B. Householder
Confidentiality Integrity	Number of incidents related to inadequate employee training or awareness programs regarding the acceptable use of information assets.	0	Acceptable Use Policy	B. Householder
Confidentiality Integrity	Number of incidents related to unauthorized access into the system.	0	Access Control Policy	B. Householder
Confidentiality Integrity	Number of times unwanted traffic passed the firewall.	0	Access Control Policy	B. Householder

Confidentiality Integrity	Number of internal access control review per year.	4	Access Control Policy	K. Sardone B. Householder
Integrity	Number of incidents arising from failed security controls built into the system.	0	Change Management and Secure Development/Engineering Policy	B. Householder
Confidentiality Integrity	Number of incidents related to unauthorized access to information on desks, printers, photocopiers, fax machines, work stations, etc.	0	Highwire Clear Desk and Clear Screen Policy	K. Sardone
Integrity Availability	Number of unsuccessful backup tests.	0	Highwire Data Backup Policy	B. Householder
Integrity	Number of completed QA/QC checks	100% of requested checks	Highwire Data QA/QC Policy	K. Sardone

Confidentiality	Number of incidents related to document errors, including but not limited to, incorrect level of confidentiality and versioning errors.	0	Highwire Document & Information Control Policy	K. Sardone
Confidentiality	Number of incidents related to unencrypted data.	0	Highwire Encryption Policy	B. Householder
Integrity	Number of weaknesses or incidents which were not reported to authorized persons.	0	Highwire Incident Management Policy	B. Householder
Integrity	Number of incidents which were not treated appropriately.	0	Highwire Incident Management Policy	B. Householder
Integrity	Number of violations of security rules that required that the disciplinary process was invoked.	0	Highwire Incident Management Policy	B. Householder

Integrity	Incident response volume in a 4-month period.	90% less than the previous quarter	Highwire Incident Management Policy	B. Householder
Integrity	Average time to detect an incident in a 4-month period.	0	Highwire Incident Management Policy	B. Householder
Integrity	Average time to correct an incident in a 4-month period.	0	Highwire Incident Management Policy	B. Householder
Integrity Availability	Cumulative down time of the system in a 4-month period.	0	Highwire Incident Management Policy	B. Householder
Integrity	Number of incidents that resulted in a change to the Risk Assessment and Risk Treatment table.	0	Highwire Incident Management Policy	B. Householder, K. Sardone
Integrity	Number of times the Risk Assessment and Risk Treatment table was reviewed in a 12-month period.	2	Highwire Risk Assessment and Risk Treatment Methodology.	B. Householder, K. Sardone

Integrity	Percent of employees who have a role in disaster recovery and/or business continuity who are familiar with their responsibilities.	100%	Highwire Disaster Recovery and Business Continuity Manual	K. Sardone
Integrity	Number and type of audits conducted from January to January.	2	Highwire Internal & External Audit Policy	B. Householder
Confidentiality Integrity	Number of penetration tests conducted by a qualified 3rd party in a 12-month period.	1	Highwire Internal & External Audit Policy	B. Householder
Confidentiality Integrity	Number of audits for compliance with PCI DSS by a qualified 3rd party in a 12-month period.	1	Highwire Internal & External Audit Policy	B. Householder
Integrity	Number of corrective actions identified during an internal audit.	0	Highwire Internal & External Audit Policy	B. Householder,

Integrity	Percent of corrective actions successfully closed out after an internal audit.	100%	Highwire Internal & External Audit Policy	B. Householder
Confidentiality Integrity	Number of incidents related to misuse of passwords by unauthorized persons	0	Highwire Password Policy	B. Householder
Confidentiality Integrity	Number of incidents related to inadequate handling of passwords.	0	Highwire Password Policy	B. Householder
Confidentiality Integrity	Number of 3rd party pentest performed annually.	1	Highwire Pentest Requirements Policy	K. Sardone B. Householder
Integrity	Percent of employees who completed ISMS training in a 12-month period.	100%	Highwire Employee Handbook	K. Sardone

Integrity	Percent of employees who know where to access the ISMS supporting documentation?	100%	Highwire Employee Handbook	K. Sardone