INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) MANUAL- SYSTEM CONTROLS

ISO/IEC 27001:2022

DOCUMENT CONTROL

DOCUMENT INFORMATION

Document Name	ISMS Manual – System Controls	
Document Filename	SYXMXNAT ISMS 002 ISMS Manual – System Controls v5.1	
Document Owner	In alignment with parent company document FISMM002	
Approved by	William Greenwood	Date: 13/04/2026
Published by	William Greenwood	Date: 13/04/2026

REVISION HISTORY FROM FRIEGHTWAYS VERSION

Version	Date	Author	Description of changes
0.1	20/06/2019	Paul Conway	Separation of Annex Policy and Procedure, Information from ISMS documentation.
0.2a	18/09/2019	Paul Conway	Updates to document references and physical location information.
1.0	01/11/2019	Paul Conway	V1.0 published
1.1	08/06/2020	Paul Conway	Amendments due to PRT DC
1.1	27/07/2020	Paul Conway	Updated special interest goods
1.1	02/09/2020	Paul Conway	V1.1 published
1.2	10/06/2021	Neill Evans	Removed references
1.3	10/08/2021	Paul Conway	Updated backup solution details
1.4	01/09/2021	Matthew Cocker	Reviewed minor revisions
1.4	03/09/2021	Paul Conway	V1.1 published

REVISION HISTORY FOR SHRED-X/ MED -X

Version	Date	Author	Description of changes
0.1	15/07/2020	Debbie Costin	New document to align to Freightways policies
1.0	22/07/2020	Debbie Costin	V1.0 published
2.0	13/06/2022	Debbie Costin	V2.0 published Major review
3.0	27/07/2023	Will Greenwood	V3.0 published Major review
4.0	02/09/2024	Charles Scheuber	V4.0 Annual Review
5.0	15/05/2025	Will Greenwood	V5.0 Updated to meet the requirements of ISO 27001 2022
5.1	13/04/2026	Matthew Dymock	Annual Review

SUPPORTING DOCUMENTATION/ REFERENCES

Shred-X ISMS Manual 1 v7.1 042026, Shred-X Statement of Applicability April 2026, ISO/IEC 27001:2022 – Information Security Management System Requirements ISO/IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection Code of Practice for Information Security Controls

TABLE OF CONTENTS

Document Control 2
Document Information 2
Revision History from Freightways version 2
Revision History for Shred-X/ Med -X 2
Supporting Documentation/ References 2
A5 Organisational Controls 6
Policies for information security 6
Information Security Roles and Responsibilities 6
Segregation of Duties 6
Management Responsibilities 6
Contact with Authorities 6
Contact with Special Interest Groups & Threat Intelligence 6
Information Security in Project Management 7
Inventory of information and other associated assets 7
Acceptable use of information and other associated assets 7
Return of assets 8
Classification of information 8
Labelling of information 8
Information transfer 8
Access Control 8
Identity Management 8
Authentication Information 9
Access Rights 9
Information Security in supplier relationships & Addressing Information Security Within Supplier Agreements 9
Managing information security in the ICT supply chain 10
Monitoring, review and change management of supplier services 10
Information security for use of cloud services 10
Information security incident management planning and preparation 10
Assessment and decision on information security events 10
Response to information security incidents 11
Learning from information security incidents 11
Collection of evidence 11
Information security during disruption 11
ICT readiness for business continuity 11

Identification of legal, statutory, regulatory and contractual requirements 11
Intellectual property rights 12
Protection of records 12
Privacy and protection of PII information 12
Independent review of information security 12
Compliance with policies and standards for information security 12
Documented operating procedures 12
A6 People Controls 13
Screening 13
Terms and conditions of employment 13
Information security awareness, education and training 13
Disciplinary process 13
Responsibilities after termination or change of employment 13
Confidentiality or non-disclosure agreements 14
Remote working 14
Information security event reporting 14
A7 Physical Controls 15
Physical security perimeter 15
Physical entry controls 15
Securing offices, rooms and facilities 15
Physical security monitoring 15
Protecting against physical and environmental threats 15
Working in secure areas 16
Clear desk and clear screen 16
Equipment siting and protection 16
Security of assets off-premises 16
Storage media 16
Supporting utilities 17
Cabling security 17
Equipment maintenance 17
Secure disposal or re-use of equipment 17
A8 Technological Controls 18
User endpoint devices 18
Privileged access rights 18
Information access restriction 18
Access to source code 18
Secure authentication 18

Capacity Management 19
Protection against malware 19
Management of technical vulnerabilities 19
Configuration management 19
Information deletion 20
Data masking 20
Data leakage detection 20
Information backup 20
Redundancy of information processing facilities 20
Logging 20
Monitoring Activities 21
Clock synchronisation 21
Use of privileged utility programs 21
Installation of software on operational systems 21
Networks security 21
Security of Network Services 21
Segregation of networks 21
Web filtering 22
Use of cryptology 22
Secure development life cycle 22
Application security requirements 22
Secure system architecture and engineering principals 22
Secure coding 22
Security testing in development and acceptance 22
Outsourced development 22
Separation of development, test and production environments 23
Change management 23
Test information 23
Protection of information systems during audit testing 23