Juniper Group Back-Up Policy

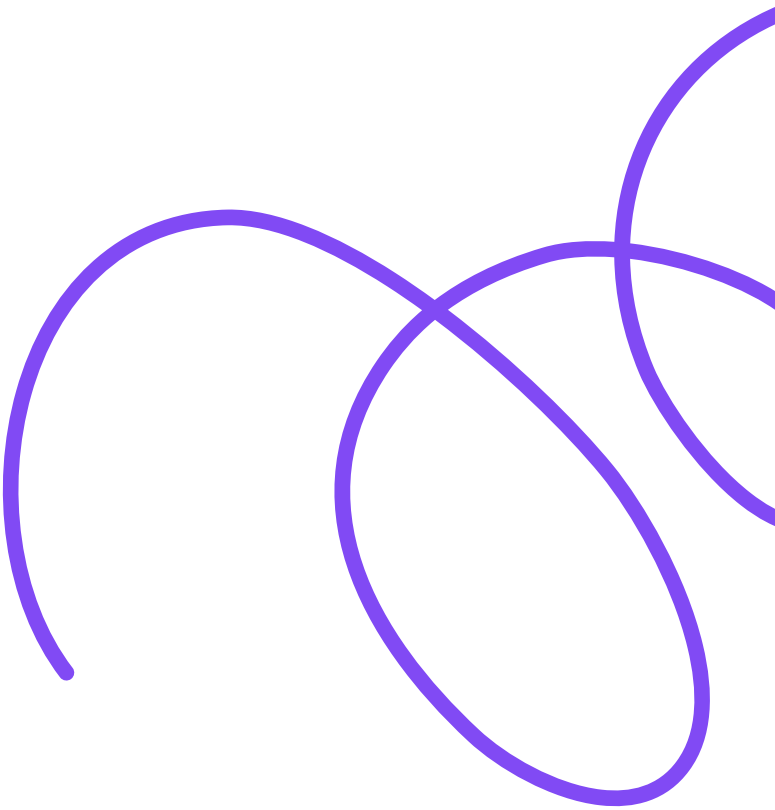
Owner: Chief Technical Officer

Version: 2.0

Date: 29/09/2025

Juniper

Contents



Version Control

Version	Date Last Modified	Last Modified By	Document Changes
2.0	24/09/2025	Group IT Manager	Addition of Group IT information.

Management of Back-Ups

Purpose

The purpose of this policy is to protect against loss of data and enable recovery from loss of data or systems.

Scope

All employees, contractors and third-party service providers.

Company owned, managed, and controlled information and systems that form part of systems and applications deemed in scope by the ISO 27001 scope statement including:

- Servers
- Databases
- Code Repositories
- Test Environments
- Development Environments
- All devices enrolled in MS Office 365

Principle

Information is backed up securely in line with the

- data retention requirements
- business requirements
- business continuity requirements and plans
- business impact assessment
- legal and regulatory requirements including but not limited to the UK and EU GDPRs and UK Data Protection Act 2018.

Back-Up Restoration Procedures

Back-up and restoration procedures are documented, in place and maintained.

Back-Up Security

Backups are encrypted using vendor built in encryption to industry standard AES-256.

Backups are stored in cloud-based solutions that as a minimum are ISO 27001 certified.

Where backup is to physical media, it

- meets industry standard AES-256,
- is labelled and stored securely on site with restricted, authorisation required perimeter access control.
- The media is transferred by an approved third party secure courier and stored in a remote secure location.

Back-Up Schedule

A back-up schedule, retention schedule and testing schedule are available and summarised as

- Point-in-time back-ups for last 7 days.
- Daily back-ups are maintained for 30 days.
- Monthly back-ups are maintained for 12 months.

Products with different back-up schedule can be found in Appendix 1.

Back-Up Testing and Verification

Back-ups of systems are tested at least annually to ensure they can be relied upon in an emergency and meet the needs of the business continuity plans and business requirements.

Back-up logs are produced and checked for errors and performance at least weekly. Where errors are found corrective action is taken.

Back-up testing log reviews are recorded.

Policy Compliance

Compliance Measurement

The ISMS Management Review Team will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by ISMS Management Review Team.

Non-Compliance

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

Review

The policy is updated and reviewed as part of the continual improvement process.

Areas of the ISO27001 Standard Addressed

ISO27001:2022	ISO27002:2022	ISO27001:2013/2017	ISO27002:2013/2017
ISO27001:2022 Clause 5 Leadership	ISO27002:2022 Clause 5 Organisational Controls	ISO27001:2013/2017 Clause 5 Leadership	ISO27002:2013/2017 Clause 5 Information security policies
ISO27001:2022 Clause 5.1 Leadership and commitment	ISO27002:2022 Clause 5.1 Policies for information security	ISO27001:2013/2017 Clause 5.1 Leadership and commitment	ISO27002:2013/2017 Clause 5.1 Management direction for information security
ISO27001:2022 Clause 5.2 Policy	ISO27002:2022 Clause 5.4 Management Responsibilities	ISO27001:2013/2017 Clause 5.2 Policy	ISO27002:2013/2017 Clause 5.1.1 Policies for information security
ISO27001:2022 Clause 6.2 Information security objectives and planning to achieve them	ISO27002:2022 Clause 5.36 Compliance with policies, rules, and standards for information security	ISO27001:2013/2017 Clause 6.2 Information security objectives and planning to achieve them	ISO27002:2013/2017 Clause 5.1.2 Review of the policies for information security
ISO27001:2022 Clause 7 Support	ISO27002:2022 Clause 5.29 Information security during disruption	ISO27001:2013/2017 Clause 7 Support	ISO27002:2013/2017 Clause 7 Human resource security
ISO27001:2022 Clause 7.3 Awareness	ISO27002:2022 Clause 5.30 ICT readiness for business continuity	ISO27001:2013/2017 Clause 7.3 Awareness	ISO27002:2013/2017 Clause 7.2.1 Management Responsibilities
ISO27001:2022 Clause 7.5.3 Control of documented information	ISO27002:2022 Clause 5.37 Documented operating procedures	ISO27001:2013/2017 Clause 7.5.3 Control of Documented Information	ISO27002:2013/2017 Clause 7.2.2 Information security awareness, education, and training
	ISO27002:2022 Clause 6 People Controls		ISO27002:2013/2017 Clause 7.2.3 Disciplinary process
	ISO27002:2022 Clause 6.3 Information security awareness, education, and training		ISO27002:2013/2017 Clause 12 Operations Security
	ISO27002:2022 Clause 6.4 Disciplinary process		ISO27002:2013/2017 Clause 12.1 Operational procedures and responsibilities
	ISO27002:2022 Clause 8 Technological Controls		ISO27002:2013/2017 Clause 12.1.1 Documented operating procedures
			ISO27002:2013/2017 Clause 12.3 Backup
			ISO27002:2013/2017 Clause 12.3.1 Information Backup

	ISO27002:2022 Clause 8.13 Information Backup ISO27002:2022 Clause 8.14 Redundancy of Information Processing Facilities		ISO27002:2013/2017 Clause 17 Information security aspects of business continuity management ISO27002:2013/2017 Clause 17.1 Information security continuity ISO27002:2013/2017 Clause 17.1.1 Planning information security continuity ISO27002:2013/2017 Clause 17.1.2 Implementing information security continuity ISO27002:2013/2017 Clause 17.1.3 Verify, review, and evaluate information security continuity ISO27002:2013/2017 Clause 17.2 To ensure availability of information processing facilities. ISO27002:2013/2017 Clause 17.2.1 Availability of information processing facilities

Appendix 1

*product is legacy system with planned end of life in next 12 months.

Product	Point in time	Daily	Monthly	Description
PupilAsset*	30 days (RDS)	365 Days (RDS) 30 days (EBS Snapshot)	-	
Horizons*	35 days (RDS)	365 Days (RDS) 30 days (Media Snapshot)	-	
Sonar	7 days	-	6 Months (weekly)	Database in Azure SQL
Insights	-	7 days	-	Database (Azure Postgres)
Sisra Analytics	-	7 days (VMs) 35 days (DBs)	-	
Sisra Observe	-	7 days (VMs) 35 days (DBs)	-	
Juniper CPD	-	2 days (Instant Rec.) 30 days (daily)	-	
OTrack*	-	31 days (every 6 hrs, App services) 7 days (DBs)	-	
JuniperWebsites	-	28 days (every 2 hrs 8am-8pm, DBs) 14 days (Media))	2 Months (DBs/Media)	
Primarysite*	-	183 Days (DBs) 1 day (GCP Sync	-	

		– Versioned, Media) 30 days (Themes)		
OTrack*	-	31 days (every 6 hrs, App services) 7 days (DBs)	-	
Catalyst*	30 days (SQL Server DBs) 35 days (DBs MySQL)	30 days (VMs)	-	
Jane*	30 days (DBs SQL Server)	30 days (VMs Portal) 7 days (VMs app)	-	
Kanban*	-	-	-	Front end webservice with API interface for Catalyst backend
MarvellousMe (Mme)*	-	35 days AWS RDS Aurora/Snapshot	-	
Target Tracker*	35 days (DBs)	16 weeks (DBs) 31 days (6 hourly, app services)	Week 31, 1 Year (DBs)	
SharePoint	-	3 years	-	Veeam SaaS Managed Service
MS Team group Chats	-	3 years	-	Veeam SaaS Managed Service
OneDrive	-	3 years	-	Veeam SaaS Managed Service
Exchange (Email)	-	3 years	-	Veeam SaaS Managed Service

Note 1: Kanban uses both Catalyst and Jane databases to provide application data. Kanban Backup Schedules are determined using the lower value recorded for source product backup schedules.

Juniper

WE LOOK AFTER YOU, SO THAT YOU CAN LOOK AFTER OUR CHILDREN