



## Due Diligence – GDPR and Data Protection

July 2025

## Contents Page

1. Introduction	Page 3
2. Frequently asked questions	Page 3
2.1. General	Page 3
2.2. Company Security and Reliability	Page 4
2.3. Transfer of data	Page 4
2.4. Changes to the application / Services	Page 4
2.5. Measures to prevent unauthorised or unlawful processing	Page 5
2.6. Data Ownership	Page 7
2.7. Sub Processors	Page 7
2.8. Loss, destruction of, or damage to data	Page 7
2.9. Disposal of data	Page 8
2.10. Record of processing Activities	Page 8
2.11. Risk Management	Page 8
2.12. Governance & Monitoring	Page 8
2.13. Data Protection Impact Assessments	Page 9
2.14. Audits / Inspections	Page 9
2.15. What if's / Other questions	Page 9
3. Client testimonials	Page 10
4. Conclusion	Page 11
5. Signatures	Page 12

- Backup and restore policy
- Business Continuity and Disaster Recovery Plan
- Clear desk and clear screen policy
- Data protection policy
- Document control and records management procedure
- Information classification policy
- Information Security Policy
- Insurances – Marsh commercial
- List of Sub-processors
- Media handling and disposal policy
- Mobile Device policy
- Password policy
- Personal Data Breach Procedure
- ROPA\*
- Service Level Agreement
- Data Leak Prevention Policy
- Legislative Compliance (Security) Policy

## Introduction

Welcome to Ningi, where innovation meets responsibility. As a frontrunner in cutting-edge solutions, we prioritise the protection of your data in the ever-evolving digital landscape. This introduction outlines our steadfast commitment to GDPR compliance and data protection, central pillars of our corporate philosophy.

Within these pages, discover Ningi's strategies for data governance, risk management, and GDPR compliance. In time, we aim to not only meet regulatory standards but surpass them, ensuring the security and privacy of sensitive information.

We recently achieved our ISO 27001 certification, which is a great milestone for a data driven company such as ours. This due diligence document is still a work in progress, reflecting our dedication to transparency, providing insights into our proactive measures and inviting stakeholders to join us on this journey.

## Frequently Asked Questions

### 1.1. General

QUESTIONS		RESPONSE
1	Ningi Description of services	The provision of financial planning software (SaaS contract) to facilitate regulated financial advice (under the advice permissions of each respective client). This can include the development of tailored software solutions, data migration and consultation where necessary.
2	Ningi Company Details	Company name: Ningi Ltd Registered office address: 60 Station Road, Nassington,

		Peterborough, England, PE8 6QB Companies House registration number: 13363671
3	Name / contact details of the person who is responsible for Ningi's information security / data protection obligations.	Internal Name: Jym Brown Contact details: <a href="mailto:jym@ningi.co.uk">jym@ningi.co.uk</a> Additionally we have engaged "Evalian" as an external DPO: Name: Evalian Ltd Email address: <a href="mailto:DPO@evalian.co.uk">DPO@evalian.co.uk</a> Telephone number: 03330 500 111
4	Is Ningi registered under the Data Protection Act with the Information Commissioner's Office?	Yes – registration number ZB098889
5	Is Ningi certified under the Information Security Standard ISO27001 or accredited to any other security related standard or Code?	Yes, Ningi is ISO 27001 certified and Cyber Essentials+ Certified.
6	Does Ningi have a security policy in place in respect of the handling of personal data?	Yes – we have an information security policy as well as a Data Protection policy which highlight's Ningi's approach to data protection and employee conduct.
7	Does Ningi have a clear desk policy in place?	Yes - Clear desk and clear screen policy
8	Does Ningi offer a service level agreement for their services?	Yes - Service Level agreement

### 1.2. Company Security and Reliability

QUESTIONS		RESPONSE
1	How is Ningi Funded?	To date, Ningi has raised circa £1.6m in funding through Haatch Ventures as a principal investor and a collection of strategic angel investors. Ningi has also been a revenue generating business since its inception, which is rare for a VC backed entity.
2	Who are the financial stakeholders / shareholders?	In addition to the above, Ningi staff and several other strategic investors are the main stakeholders / shareholders.
3	What risks does Ningi have with its financial structure and how are these mitigated?	Ningi possesses similar risks to any other VC / Angel backed tech business, but with some differences. Our choice of partnerships ensures strong long-term financial backing, along with potential capital raising events should the situation arise. We have several contingencies in place in order to modify the business strategy in light of market changes or client successes. We also have the option of conducting a series A raise in the near future to consolidate our position.

### 1.3. Transfer of data

QUESTIONS		RESPONSE
1	Does Ningi Process data outside of the UK	No

	and EU?	
2	Does Ningi have safeguards in place at each location where data will be processed?	Yes – secure cloud servers are used.
3	Can Ningi ensure the rights and freedoms of the data subjects are adequately protected at each location and whilst data is 'in transit'?	Yes, using https

#### 1.4. Changes to the application / Services

QUESTIONS		RESPONSE
1	Approximately, how often does Ningi make upgrades to the application / services?	We run daily updates
2	Will these upgrades impact the use of your services?	No
3	How and when will you notify clients about any scheduled maintenance?	At least 24 hours' notice would be given via email. We aim to limit downtime to be outside of working hours.

#### 1.5. Measures to prevent unauthorised or unlawful processing

QUESTIONS		RESPONSE
1	What category of data will be processed? (eg: personal data or special category personal data or both)	Data processed is in accordance with data collected by the respective client for the purposes of financial advice, including personal and special category data.
2	What computer operating system measures are in place to protect data?	Mobile Device Management (Kandji) See appendix for password policy
3	What measures are in place to prevent unauthorised access to data from outside hackers (i.e. firewalls) and to what extent is the adequacy of current precautions monitored?	Firewalls managed by Kandji to ensure that only designated traffic is authorised. We also use Bitdefender which is a cyber security threat prevention and detection system (anti malware).
	Is there a formal policy on this?	Ningi has a strict Access Control Policy as validated by the ISO 27001 certification process.
4	Does Ningi enter into contracts with third parties for the provision of services which may involve intended or accidental access to our data, for example, software maintenance?	No
5	Would Ningi ever be required to allow data, which you have agreed to process (or copies of it) to leave your premises? If so, please specify why and what precautions you take to prevent unauthorised access to, loss of, or destruction or corruption of data.	See appendix for media handling and disposal policy.
6	Where data is held in manual form, is it / will it be identified in any way as being confidential data belonging to us?	Yes - Only in the event of receipt of manual data as Ningi does not practise the manual creation of client data. See appendix for policy.
	Will manual data be kept secure at all times?	See above
7	Does Ningi carefully screen all employees who may have access to data to ensure they	Yes. Ningi has a recruitment policy which ensures all staff are screened / vetted before hiring. Internally,

	are trustworthy?	only minimal staff have any level of access to client data.
8	Are all staff informed of their responsibilities in keeping data secure in accordance with our requirements?	Yes, all staff must read the Staff Security Policy as part of their induction.
	Do such employees sign confidentiality undertakings?	Yes - Confidentiality agreement is part of staff contracts
9	Are the employees trained as to the issues arising in the context of information security? For example, are they made aware not to leave terminals unattended without logging out where data could be accessed by unauthorised personnel?	Yes, all staff must read the Staff Security Policy as part of their induction. GDPR and other training is provided. Also see appendix for Data Protection Monitoring Policy & Checklist
10	Will data only be processed in a secure area?	No - Staff are permitted to work remotely where required but their devices are managed by Kandji as above.
11	What precautions are taken to ensure that non-authorised personnel cannot access the area / premises in which data is processed?	Our office is secure and not accessible to the public. Kandji enforces a screen lock where a password is required after 5 minutes, and there is a policy for staff members to lock screens when they leave their desk. Devices are taken home in the evening and kept securely.
12	How quickly can Ningi react if a security vulnerability is identified in your product / service?	We would be notified of any possible bugs or security flaws and they are dealt with within a reasonable timeframe based on the level of vulnerability and priority, but always within the same day.
13	What are your data deletion and retention timescales?	See appendix for Document control and records management procedure
	Does this include end-of-life destruction?	Yes
14	Will data be shared across other services you may offer?	No
15	What procedures does Ningi have in place to promptly address a personal data breach.	Robust Personal Data Breach Procedure, as well as a Personal data breach assessment process. Employee training in place regarding personal data breach awareness and response.
16	What procedures does Ningi have in place to promptly notify a controller of a personal data breach affecting the shared personal data?	Personal data breach procedure, as well as relevant clauses in Data Processing Agreement.
17	What procedures does Ningi have in place to assist a controller in dealing with a personal data breach affecting the shared personal data, including assisting a controller in notifying the supervisory authority and data subjects?	Personal data breach procedure, as well as relevant clauses in Data Processing Agreement.
18	What technical measures does Ningi have in place to safeguard personal data?	<p><b>Encryption:</b> Personal data is encrypted at rest and encrypted in transit</p> <p><b>Mobile devices:</b> Mobile Devices are encrypted</p> <p><b>Restricted Access:</b> The principle of least privilege is applied</p> <p><b>ISO Standards:</b> Certified September 2024</p> <p><b>Certification:</b></p>

		<p>We hold ISO 27001, Cyber Essentials and Cyber Essentials Plus Certificates</p> <p><b>Penetration Testing:</b> We conduct regular penetration testing</p> <p><b>Vulnerability Scanning:</b> We conduct regular vulnerability scanning</p> <p><b>Anti-malware:</b> We use anti-malware and ensure it is regularly updated</p>
19	Please advise of any other technical security measures you have in place to safeguard personal data and/or assist in meeting its obligations under the UK GDPR / EU GDPR (whichever is applicable) in relation to the security of processing.	<p>Ningi utilises double encryption to maintain safety. Clients are also able to download all of their data whenever required in order to meet any GDPR requirements.</p>

#### 1.6. Data Ownership

QUESTIONS		RESPONSE
1	What are Ningi's terms when it comes to ownership of data?	Ningi acts only as a processor of data with our clients being the controllers of their data.
2	How easy is it to export data from your service(s) when moving to a new service?	Exports can be run at your request if required.
3	What happens to our data if we discontinue Ningi's service(s) in the future? Do you delete all data immediately and securely?	Yes
4	Do you delete data completely if we delete it from the application?	Yes, except for back-ups.

#### 1.7. Sub-processors

QUESTIONS		RESPONSE
1	Do you use sub-processors?	Yes – see attached list of sub-processors in the appendix
2	If yes, did you follow a data protection due diligence procedure?	Yes
3	If yes, do you have UK GDPR/EU GDPR (whichever is applicable) compliant Data Processing Agreements in place with each of your processors?	Yes

#### 1.8. Loss, destruction of, or damage to data

QUESTIONS		RESPONSE
1	Does Ningi have a business continuity plan in place to deal with any interruptions to data processing?	Yes, we have a documented Business Continuity and Disaster Recovery Plan – see appendix.
2	What back-up systems are in place to prevent loss of data caused by system crashes?	We have continuous protection with rolling back-ups daily.
3	How many copies of data are backed-up?	4 days' worth
4	How often are back-ups performed?	Daily
5	What back- up systems are in place to prevent loss of data caused by fire, flood, burglaries etc.?	We use AWS
6	Is your computer equipment on which data is processed protected from power failure or electrical disturbances?	Not currently, however this is an ongoing process.
7	What virus detection / prevention software is in place?	Managed by Bitdefender and Kandji.
8	Are all areas in which data is processed suitably protected from damage by firm, flood or similar disasters?	Yes – we use AWS as above.
9	Is manual data (and disks containing data) stored in locked fireproof cabinets when not being processed?	N/A as above
10	Do you have audit trails in place to monitor who is accessing which data?	Yes - This is recorded within the application.
11	Upon request, will we be able to obtain a copy of our data in a usable format?	Yes – This could be made available within 1 month in sql export format.
12	How quickly will you be able to restore data, without alteration, from a back-up if you suffered a major data loss?	Within 1 hour.

### 1.9. Disposal of data

QUESTIONS		RESPONSE
1	Is data removed from all equipment before that equipment is disposed of?	Yes - See appendix for Media handling and disposal policy
2	How is data in manual form, disposed of?	As above

### 1.10. Record of Processing Activities

QUESTIONS		RESPONSE
1	Has your organisation prepared a ROPA or similar document which sets out the personal data your organisation processes?	Yes
2	Is your ROPA reviewed regularly and kept up to date?	Yes



### 1.11. Risk Management

QUESTIONS		RESPONSE
1	Does Ningi have a data protection risk register that is reviewed regularly and kept up to date?	YES
2	What procedures does Ningi have in place to ensure data protection risks are addressed appropriately and in a timely manner?	Risk registers regularly reviewed as well as a DPIA procedure in place to ensure any new processing/changes in processes are assessed in terms of the potential risks involved.

### 1.12. Governance and Monitoring

QUESTIONS		RESPONSE
1	Is data protection a regular agenda item at any board meetings within Ningi?	YES
2	What procedures does Ningi have in place to ensure that data protection compliance is monitored?	We use a Data Protection Monitoring Checklist

### 1.13. Data Protection Impact Assessments

QUESTIONS		RESPONSE
1	What procedures does Ningi have in place to assist a controller in meeting its obligations under the UK GDPR / EU GDPR (whichever is applicable) in relation to Data Protection Impact Assessments?	DPIA procedure in place to ensure any new processing/changes in processes are assessed in terms of the potential risks involved

### 1.14. Audits / Inspections

QUESTIONS		RESPONSE
1	What procedures does Ningi have in place to allow a controller to conduct audits and inspections in relation to your processing of the shared personal data?	Ningi will support audits by controllers where reasonably possible and make available the relevant documents.
2	What procedures does your organisation have in place to demonstrate your compliance with Article 28 of the UK GDPR / EU GDPR (whichever is applicable)?	Ningi can present evidence of compliance with all elements of the Art 28 requirements. Including a Personal Data Breach procedure and DSRR procedure

### 1.15. What if's / Other questions

QUESTIONS		RESPONSE
1	Have you ever been subject to any enquiry / investigation by the Information Commissioner?	No
2	When was your organisation last subject to an independent data protection audit / assessment?	September 2024 – No remediation required
3	What if Ningi decided to pull out (financial/personal choice/other reasons), what would happen to us a client that is fully reliant on the system for all its operations?	Client code can be placed in escrow in order to protect the integrity of their tech infrastructure and back-office functions. In addition, Ningi has strict GDPR and security procedures to protect client data including encryption and deletion of information where required.
4	What if Key employees leave, who were integral to the development roadmap, how quickly can they be replaced?	Our strategy is to recruit layers of domain specialist expertise in order to reduce reliability on any one member of staff. This is now present in both product and engineering functions and will be so shortly in operations and customer success. The product / engineering roadmap is nearing completion, meaning very little risk to future success. This is also bolstered by succession planning within each department, however this is understandably still in its infancy.
5	What if Ningi cease trading - what rights do we have to continue using the tech/platform that we have developed?	In the event of Ningi ceasing trading, code will be placed in escrow, providing the opportunity for existing clients to maintain the tech at their own cost.

## Client Testimonials

### Westminster Wealth Management: A Tailored Digital Evolution

**Overview:** Westminster Wealth Management envisioned a scaled digital proposition in the workplace and partnered with Ningi for a holistic tech solution right from the inception.

**The Challenge:** Embarking on a venture that required not just tech proficiency but regulatory adroitness and a flexible partnership.

**How Ningi Delivered:** Ningi played a multifaceted role, providing a myriad of services ranging from scoping, design, documentation, marketing, branding, and even regulatory communications with the FCA. This collaboration wasn't just about building tech; it entailed securing insurances, adhering to ISO27001 standards, and working on extensive documentation for FCA's innovation pathways. Moreover, the project required stringent due diligence and approvals, given its association with local government councils.

One key aspect was the full robo investment advice journey. Ningi deciphered the complexity of the task, partnered with ATR profiling and AML suppliers, and seamlessly integrated everything.

**Outcome:** Ningi, using a mix of strategic sessions and execution prowess, brought James Anderson's vision to life. The success is best encapsulated in James' words: "We looked at over a dozen potential suppliers for a digital advice engine. Ningi was the only one offering a bespoke solution that evolved over time. Our aim was online guidance for AVC scheme fund choices, and Ningi echoed our future vision." This 12-month project, now moving to a phase of enhanced collaboration, mirrors the proposal outlined, underpinning

Ningi's consistent model of MVP development, iteration, and scaling.



### **Ellis Bates: Testament to Ningi's Maturity & Reliability**

**Overview:** Ellis Bates, a prestigious financial firm with a vast footprint across the UK, sought a robust practice management solution, placing their trust in Ningi after a comprehensive vendor assessment.

**The Challenge:** To provide an all-encompassing tech suite for a business with over 100 employees, managing a myriad of tasks from client interaction to internal processes.

**How Ningi Delivered:** Ningi demonstrated its capability to handle extensive operations, deploying solutions that managed client portals, back office CRM, income reconciliation, and intricate reporting. This wasn't just about technical delivery; it was a testament to Ningi's operational maturity and the ability to handle the demands of a large-scale, well-established financial firm.

**Outcome:** Ellis Bates, with thousands of clients relying on them, needed reliability and efficiency. Ningi stood up to the task, implementing their core front and back office tech seamlessly. This case underscores Ningi's readiness not just for start-ups and mid-scale ventures but for industry bigwigs, reflecting the scalability and adaptability of Ningi as a tech partner.

### **Testimonials:**

1. <https://www.linkedin.com/feed/update/urn:li:activity:7091704068724678657>
2. <https://www.linkedin.com/feed/update/urn:li:activity:7086614771625512960>

## **Conclusion**

In concluding this Due Diligence document, Ningi reaffirms its unwavering commitment to data protection, transparency, and the highest standards of GDPR compliance. We recognise the evolving landscape of

digital innovation and the paramount importance of safeguarding the sensitive information entrusted to us by our clients.

Our comprehensive strategies outlined in this document reflect not only our dedication to meeting regulatory standards but our proactive stance in surpassing them. We are very proud to have achieved ISO 27001 certification and invite our stakeholders to join us on this continued journey, marked by a culture of integrity, accountability, and continuous improvement.

At Ningi, we prioritise your data security and privacy. We strive not only to comply with industry standards but to set new benchmarks in data protection, demonstrating our responsibility as a leading player in the digital age. As we progress, we remain open to feedback and collaboration, recognising that our journey is a shared one.

## Signatures

Signed on behalf of Ningi:



**Print Name: Jym Brown**

**Role: Chief Operating Officer**

**Date: 03/06/2025**

## Appendix:

Welcome to our compilation of policies and procedures—a living document that reflects our ongoing commitment to our ISO 27001 certification. In here, you'll find various policies, some still in draft form, all undergoing regular reviews to meet evolving standards.

For simplicity, we've skipped detailed document control tables for each policy. However, if you need them, just let us know and we can make these available for you. The documents are in alphabetical order but if you click the policy you'd like to view below, it'll take you straight to it, to save lots of scrolling!

- ✓ Backup and restore policy
- ✓ Business Continuity and Disaster Recovery Plan
- ✓ Clear desk and clear screen policy
- ✓ Data Leak Prevention Policy
- ✓ Data protection policy
- ✓ Document control and records management procedure
- ✓ Information classification policy
- ✓ Information Security Policy
- ✓ Insurances – Marsh commercial
- ✓ Legislative Compliance (Security) Policy
- ✓ List of Sub-processors
- ✓ Media handling and disposal policy
- ✓ Mobile Device policy
- ✓ Password policy
- ✓ Personal Data Breach Procedure
- ✓ ROPA\*
- ✓ Service Level Agreement

## Backup and Restore Policy

### Purpose

The purpose of this policy is to set out the requirements for backup and recovery of Ningi's electronic and physical information to keep data safe in the event of events such as:

External Threats e.g., natural disaster, flood, fire, cyber-attack on the main data centre.

Accidental or wilful deletion of a file by an employee.

### Applicability

This policy applies to the IT Function.

### Policy

Backups of data stored in all Ningi systems will be maintained and tested to ensure business continuity in the event of disaster. Without complete and usable backups, the organisation is exposed to an unacceptable level of risk and may be subject to significant legal consequences.

### Roles and Responsibilities

The CTO is responsible for ensuring the effectiveness of this Backup and Restore Policy and for ensuring that regular tests are conducted.

### Ningi Managed Systems

Being a Cloud-Based company, Ningi does not hold any data on its infrastructure (including Laptops) and relies on cloud providers' backups.

### **Local Machines**

All business correspondence, documentation and intellectual property should be stored on the appropriate Cloud systems, e.g. SharePoint, Teams or the source control system. Local machines should not be relied upon for storing any business-related data.

### **Backup Schedule**

The backup schedule for each Ningi managed system must be designed and meet the continuity requirements of the organisation.

In all cases, failed backups must be reported, investigated, and repeated as soon as practicable.

### **Restores**

Ningi shall ensure the integrity of its backups by selecting appropriate technology, and frequency and location of backups. Ningi may at times verify the integrity of its backups by scheduling and running full or partial restores. Restore activities will be subject to change control.

### **Cloud Service Providers**

Cloud system backups depend on the split of shared security (including system and data availability) responsibility between the Cloud Service Provider ("CSP") and Ningi. This split of responsibilities will depend on the type of the cloud service provided, covering SaaS, PaaS and IaaS.

The CSP will typically be responsible for data backup from SaaS and PaaS and Ningi will typically be responsible for data backups from apps and services hosted using IaaS service (because these will be Ningi managed systems). Some SaaS, including M365 apps, provide versioning of files which allows Ningi users to 'roll back' to an earlier version of a file.

Ningi shall validate that the CSPs it uses for SaaS and PaaS services backup Ningi data stored on their systems and keep a record of the backup practices provided by each SaaS and PaaS vendor.

### **Compliance and Monitoring**

Compliance with this and all other policies and procedures is mandatory.

Any breach of policy may result in disciplinary action, up to and including dismissal.

### **Monitoring**

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

### **Audit and Review**

#### **Internal Review**

Compliance with this policy will be monitored through Information Security Internal Audits, and by other management checks as required.

### **External Review**

Inspections by external auditors may be carried out from time to time.

As part of these activities, external inspectors may ask to view internal records. Supervised access to such records must be provided where requested.

Copies of records must not be removed from site by an inspector unless this has been specifically approved by the ISMS Manager.

### **Policy Review**

This policy will be reviewed by the ISMS Manager or his nominated delegate at regular intervals, not exceeding 1 year, or when business changes warrant it as part of the continual improvement process.

## **Business Continuity & Disaster Recovery**

### **Disaster recovery**

Ningi's products and services are entirely cloud based, relying on cloud/remote technology such as Heroku, AWS, Github and Basecamp for operations.

All staff are well equipped to work remotely, without compromise to data security or service provision. In the event of a disaster affecting our third-party cloud service providers, any disruption will be closely monitored by Engineering and the service provider switched if the issue persists past 24 hours, where possible.

MongoDB Atlas uses replica sets with at least 3 servers within the same data centre to provide redundancy and high availability.

### **Data backup and retention**

Our MongoDB Atlas hosting service provides secure backups that are run daily and are secured to storage between 2 days and 12 months. Atlas encrypts the storage engine of all snapshot volumes, ensuring the security of cluster data at rest.

The default backup frequencies and retention periods can be found here:

#### Back Up Your Database Deployment

Client data is stored in separate databases, with distinct backups for each client. Snapshots are available on request and will be manually requested through the Cloud backup system. Atlas takes on-demand snapshots immediately, unlike scheduled snapshots which occur at regular intervals. If there is already an on-demand snapshot with a status of queued or inProgress, we must wait until Atlas has completed the on-demand snapshot before taking another.

## **Certified and secure data erasure**

Backups are taken to cloud storage and deleted upon contract/service closure. MongoDB Atlas guarantees secure deletion across their storage platforms.

## **Distributed Denial of Service (DDoS) protection**

MongoDB Atlas is physically very secure and Ningi employs a layer of 3rd party services to prevent unauthorised access.

Only key Ningi service personnel have access to our operating system and your data. No other parties have access to client data. This access is password protected through an end-to-end encryption password manager called 1Password:

[1Password - Password Manager for Families, Businesses, Teams | 1Password](#)

Ningi have no physical access to data. We use cloud services that use the AWS ecosystem to mitigate this issue. Any data we store has all the physical protections afforded by AWS.

Ningi rely on the technical controls provided via our cloud service providers. Only personnel with critical access will be able to manage deployments and have access to data.

## **Security patches & updates**

Ningi regularly reviews servers for critical security patches and updates. Most patches can be implemented without downtime and any that require such will be discussed with the client. As the service is deployed as SaaS (Software as a Service), patches, firmware upgrades etc. are automatically deployed by MongoDB Atlas without service impact.

## **Testing**

Testing is scheduled twice annually in November and May.

Testing will simulate:

1. Inability to access home office (laptop and place of work)
2. Cloud service provider failure.



## Clear Desk and Clear Screen Policy

### Introduction

This policy documents Ningi's commitment to ensuring that employee, client, supplier and corporate information is viewed only by people who have authority to do so.

### Applicability

This policy applies to all staff, including employees, contractors and interns working for or under the control of Ningi.

### Principles

This Clear Desk and Screen Policy provides guidelines to reduce the potential risks involved in:

- Information security.
- Physical security.
- Confidentiality.
- Data protection.
- Fraud.

The main reasons for the introduction of this policy are to:

- Ensure that Ningi complies with applicable Data Protection laws and regulations.
- Enable the company to protect its employees', its clients' and its suppliers' information by adhering to appropriate procedures regarding confidentiality.
- Reduce the chances of a security breach, both with regards to the physical security of the office and the security of Ningi's network and tools.
- Demonstrate Ningi's commitment to the protection of personal, corporate, client and supplier data, which falls under its overall Information, ICT and Data Protection policies.

### The Policy in Operation

The policy should become part of everyday routine within the individual's general office and housekeeping responsibilities. The key areas covered by this policy are:

- Desks and working areas.
- Computer screens.
- Notice boards.
- Printers.

### Desk and Working Areas

Ningi follows paperless principles and no Ningi information should be printed in the office or at home.

All confidential paperwork, notebooks, documentation, etc. shall be put away in a lockable drawer or cabinet overnight and when you are away from your desk.

No confidential paperwork, notebooks, documentation, etc. shall be left unattended in working areas such as meeting and conference rooms.

Any printed material that contains personal or confidential information shall be securely disposed of as soon as it is no longer required.

### **Computer Screens**

Documents that are open on computer monitors pose a security risk around the areas outlined above.

If staff leave their desk at any time, all devices must be locked manually.

Ningi does not enforce an automated timeout of all devices and user sessions, however it is recommended that the laptop screen timeout setting should not be longer than 5 minutes.

Any mobile phone used for work purposes must be locked when not in use; (in the event that staff use company devices, this should be more than a recommendation and should be enforced via group policy).

At the end of each working day, staff shall log out of systems and their computer must be shut down and taken home.

### **Notice Boards and White Boards**

It is the responsibility of all staff to ensure that notice boards and white boards are kept in good order and to remove out of date or sensitive material.

Notice boards and white boards must be protected from unauthorised viewing, for example, from visitors or during video calls.

### **Printers**

As noted above, Ningi operates as a paperless organisation and no confidential documentation should be printed.

Documents shall only be printed when it is absolutely necessary for hard copies to be made available;

Printed documents shall be collected from printers as soon as available.

Documents labelled as 'Internal' or 'Confidential' found to have been left uncollected on printers should be disposed of securely.

### **Compliance and Monitoring**

- Compliance with this and all other policies and procedures is mandatory.
- Any breach of policy may result in disciplinary action, up to and including dismissal.

### **Monitoring**

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

## **Audit and Review**

### **Internal Review**

Compliance with this policy will be monitored through Information Security Internal Audits, and by other management checks as required.

### **External Review**

Inspections by external auditors may be carried out from time to time.

As part of these activities, external inspectors may ask to view internal records. Supervised access to such records must be provided where requested.

Copies of records must not be removed from site by an inspector unless this has been specifically approved by the ISMS Manager.

### **Policy Review**

This policy will be reviewed by the ISMS Manager or his nominated delegate at regular intervals, not exceeding 1 year, or when business changes warrant it as part of the continual improvement process.

## **Data Protection policy**

### **Introduction**

This Data Protection Policy (this “policy”) sets out the obligations of Ningi (“Ningi”, “we”, “us”, “our”) regarding data protection and the rights of individuals whose Personal Data we collect, use and process in the course of our business activities.

This policy applies to all Ningi employees, workers and contractors (“personnel”, “you”, “your”). Your compliance with this policy is mandatory. Any breach of this policy and our other data protection policies/procedures may result in disciplinary action, up to and including termination for serious offences.

This policy has been prepared with due regard to the data protection laws applicable to Ningi and our Personal Data Processing activities. These Data Protection Laws include the UK General Data Protection Regulation (“UK GDPR”) and / or the EU General Data Protection Regulation (“EU GDPR” - EU Regulation 2016/679) (whichever is applicable) and the Data Protection Act 2018 (“DPA 2018”), (collectively referred to as the “Data Protection Law”).

This policy should be read together with the following related documents:

- Ningi Data Protection by Design & Default Policy
- Ningi Personal Data Retention and Destruction Policy
- Ningi Information Security Policy
- Ningi Data Subject Rights Procedure

- Ningi Personal Data Breach Procedure
- Ningi DPIA Procedure
- Ningi TIA template
- Ningi Data Protection Monitoring Framework Guidance

## Policy Statement

Ningi places high importance on respecting the privacy and protecting the Personal Data of individuals with whom we work including our clients, end customers and employees. We are committed to the fair, lawful and transparent handling of Personal Data and to facilitating the rights of individuals. Our policy is to comply not only to the letter of the law, but also to the spirit of the law.

## Scope

This policy applies to all Personal Data processed by Ningi whether held in electronic form or in physical records, and regardless of the media on which that data is stored. It applies to Personal Data we process as a Data Controller and Personal Data we process as a Data Processor (on behalf of our clients).

Ningi is registered as a Data Controller with the Information Commissioner's Office having registration number ZB098889.

## Definitions

The following definitions apply across all Ningi data protection policies, procedures and supporting documents:

Term	Description:
Accountability	A duty to answer to the success or failure of strategies, decisions, practices and processes.
Criminal Information	Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings
Data Controller	A person, entity or organisation that determines the purposes and means of processing Personal Data.
DPA 2018	Data Protection Act 2018
Data Protection Officer	The Data Protection Officer is responsible for overseeing data protection strategy and implementation to ensure compliance with Data Protection Law.
Data Protection Law	UK GDPR and / or the EU General Data Protection Regulation ("EU GDPR" - EU Regulation 2016/679) (whichever is applicable) and the Data Protection Act 2018 ("DPA 2018").
Data Processor	A person, entity or organisation that processes Personal Data on behalf of a Data Controller.
Data Subject	Any natural person (individual) whose Personal Data is being processed.
Data Protection Impact Assessment (DPIA)	A DPIA is designed to help an organisation assess the risks associated with data processing activities that could compromise the rights and freedoms of individuals. It can be used to identify and mitigate risk associated with a product, service, business process or other organisational change.
EU GDPR	EU Regulation 2016/679 General Data Protection Regulation
Information Commissioner's Office (ICO)	An independent public body established in the UK responsible for monitoring the application of the UK GDPR, Data Protection Act 2018 and the Privacy & Electronic Communications Regulations.
Legitimate	Determines if individual's Personal Data is being used in ways they would reasonably

Interest Assessment (LIA)	expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Personal Data	Any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Processing	Any operation or set of operations that is performed on Personal Data, such as collection, recording, organising, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, combination, restriction or erasure.
Record of Processing Activity (RoPA)	A RoPA is a requirement under Article 30 of the GDPR. This is a living document that describes the types of personal data that Ningi controls and processes.
Sensitive Personal Data	Special Category Data and Personal Data relating to criminal convictions and offences.
Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, biometric data (where used to identify a data subject), data concerning health and data concerning a natural person’s sex life or sexual orientation.
UK GDPR	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018

## Responsibilities

Key data protection responsibilities within Ningi are as follows:

- Ningi Senior Management are accountable for ensuring we meet our data protection obligations;
- the COO is responsible for implementing and enforcing this policy;
- the Management Team are responsible for ensuring that personnel under their management are made aware of adhere and to this policy;
- all personnel working with Personal Data over which they have decision making authority are responsible for ensuring it is kept securely, is accessible only to those who need to use it and is not disclosed to any third party without the authorisation of a member of the Board; and
- all personnel are required to read, understand, and adhere to this policy when processing Personal Data on our behalf.

You should speak with the COO to ask a question, or raise a concern, relating to this policy or data protection.

## Data Protection Principles

The following data protection principles shall govern the collection, use, retention, transfer, disclosure and destruction of Personal Data by Ningi :

- **Principle 1 - Fair, Lawful & Transparent** Personal Data must be processed lawfully, fairly, and in a

transparent manner in relation to the Data Subject.

- **Principle 2 - Purpose Limitation** Personal Data must only be collected and processed for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- **Principle 3 - Data Minimisation** Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Principle 4 - Accuracy:** Personal Data must be accurate and kept up to date.
- **Principle 5 - Storage Limitation:** Personal Data which permits identification of Data Subjects (i.e. data which has not been anonymised) must be kept for no longer than is necessary for the purposes for which the Personal Data are processed.
- **Principle 6 - Security:** Personal Data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- **Data Protection by Design and Default** Ningi shall ensure that the risks to rights and freedoms of Data Subjects associated with processing are key considerations when:

Designing, implementing and during the life of business practices and processes that involve the processing of personal data (“processing activities”); and  
Developing, designing, selecting, procuring, and using applications, services, products and other IT systems and technologies for collecting, holding, sharing, accessing, and otherwise processing personal data (“processing systems”).

This risk led approach to processing activities and processing systems shall apply throughout the full lifecycle of the processing, from initial planning and setting of specifications, during use of processing systems, through to disposal of the personal data. It shall take into account both the likelihood and the severity of the potential harm to the rights and freedoms of Data Subjects.

Where the risk to rights and freedoms of Data Subjects is likely to be high, or where otherwise required by law or the relevant supervisory authority, a DPIA shall be performed in accordance with our DPIA procedure.

Safeguards and preventive measures shall be implemented into processing activities and processing systems from the outset and throughout the processing lifecycle, to mitigate the risks to data subjects and protect their rights. These safeguards and measures shall be proportionate to the risks and include organisational (e.g. policy, awareness, governance, and assurance) as well as technical measures (e.g. pseudonymisation). The objectives of such safeguards and measures shall include:

- data minimisation
- limiting the extent of the processing, storage, and access to what is strictly necessary
- ensuring transparency for data subjects regarding the processing activities; and
- ensuring the security of the personal data.

## Data Processing Obligations

### Ningi as a Data Processor

Where Ningi is a Data Processor, we may only process Personal Data in accordance with the controller’s

documented instructions as set out in a data processing agreement. We may only transfer Personal Data out of the UK and the EEA and appoint sub-Data Processors as permitted by the data processing agreement.

Personal Data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Access to the Personal Data must be limited only to personnel who are subject to an obligation of confidentiality and who need access to carry out their assigned duties.

We must assist the Data Controller to meet their compliance obligations under applicable laws including for the purposes of:

- ensuring the security of processing, including by implementing appropriate technical and organisational measures;
- supporting the facilitation of subject rights of Data Subjects whose Personal Data we hold;
- enabling the Data Controller to notify the relevant supervisory authority following a Personal Data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of affected Data Subjects;
- enabling the Data Controller to notify affected Data Subjects following a Personal Data breach which is likely to result in a high risk to the rights and freedoms of affected Data Subjects; and
- supporting data protection impact assessments carried out by the Data Controller as appropriate.

Upon termination of the data processing agreement, we must delete or return Personal Data as set out at Section 13 of this policy.

We must also support the Data Controller to demonstrate Accountability and compliance with applicable laws by providing them with all information necessary to demonstrate compliance by Ningi and allow for and participate in audits by the Data Controller or their representative.

#### Ningi as a Data Controller

Where Ningi is the Data Controller, Data Subjects must be provided with information notifying them of the purposes for which Ningi will process their Personal Data (a “privacy notice”). When Personal Data is obtained directly, the privacy notice shall be provided to the Data Subject at the time of collection. When Personal Data is obtained indirectly, the privacy notice shall be provided to the Data Subject as soon as possible (and not more than one calendar month) after it is obtained from a third party. The privacy notice must explain what processing will occur and must also include the information set out at Schedule 1.

Use of the Personal Data by Ningi must match the description given in the privacy notice and be limited to what is necessary for the specific purposes stated. Where our lawful basis for processing is based on our legitimate interests, we may only process the Personal Data if our legitimate interests are not outweighed by the interests, rights and freedoms of the Data Subjects in question. A legitimate interests assessment must be performed to confirm this.

We must not collect or process any more Personal Data than is strictly necessary for the purposes of the processing (“data minimisation”), as set out in our privacy notice, and must ensure that data minimisation continues to be applied throughout the lifetime of the processing activities.

Personal Data must be kept accurate and up to date. The accuracy of Personal Data must be checked when

it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps are to be taken without delay to amend or erase that data, as appropriate. Personal Data must not be kept for any longer than is necessary for the purpose for which that data was originally collected and processed. When the data is no longer required, all reasonable steps must be taken to securely erase or dispose of it without delay, as set out at Section 13 of this policy.

Personal Data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

### **Accountability**

Only those personnel that need access to, and use of, Personal Data to carry out their assigned duties correctly will be permitted access to Personal Data we hold. All personnel handling Personal Data on behalf of Ningi must be:

- made fully aware of both their individual responsibilities and Ningi's responsibilities under this policy and applicable law, and be provided with a copy of this policy;
- appropriately trained to do so and suitably supervised, with training to be provided upon starting with Ningi and refresher training to be provided at least annually; and
- bound to handle the Personal Data in accordance with this policy and the law by contract.

The methods of collecting, holding and processing Personal Data by personnel, or other parties working on our behalf, are to be regularly evaluated and reviewed by the COO.

All consultants, agencies and other parties working on our behalf and handling Personal Data must ensure that all of their employees who are involved in the processing of Personal Data are held to the same obligations as applicable to Ningi personnel arising out of this policy.

When using a Data Processor (or, where permitted, a sub-Data Processor), a binding contract must be implemented between Ningi and the Data Processor setting out the subject matter and duration of the processing; the nature and purpose of the processing; the type of Personal Data and categories of Data Subject; and the obligations and rights of the controller. Processor contracts must also include the terms set out at Schedule 2.

Ningi will keep written internal records of processing activities in respect of all Personal Data collection, holding, and processing ("RoPA"). Where Ningi is a Data Processor, we will keep a Data Processor RoPA and where we are the Data Controller, we will keep a Data Controller RoPA.

### Data Processor RoPA

Where Ningi is a Data Processor, the RoPA will incorporate the following information:

- the name and contact details of the Data Processor and of each Data Controller on behalf of which we are acting as Data Processor;
- the categories of processing carried out on behalf of each controller;
- details of any transfers of Personal Data to countries outside the UK or European Economic Area



- (“EEA”) including all mechanisms and security safeguards;
- descriptions of the technical and organisational measures we have implemented to ensure the security of Personal Data.

#### Data Controller RoPA

Where Ningi is the Data Controller, the RoPA will incorporate the following information:

- the name and contact details of the Data Controller, its point of contact for data related concerns;
- the purposes for which we process Personal Data;
- details of the categories of Personal Data collected, held, and processed by us; and the categories of Data Subject to which that Personal Data relates;
- details (and categories) of any third parties that will receive Personal Data from us;
- details of any transfers of Personal Data to countries outside the UK or European Economic Area (“EEA”) including all mechanisms and security safeguards;
- the envisaged retention periods for the different categories of Personal Data; and
- descriptions of the technical and organisational measures we have implemented to ensure the security of Personal Data.

#### **Risk Management**

Ningi will monitor the risks to Data Subjects associated with all existing and planned Personal Data processing activities and implement appropriate technical and organisational measures to safeguard Data Subjects and ensure the data protection principles set out in this policy are met. This risk led approach to data protection will be applied across all Ningi business activities to ensure data protection by design and by default, as set out in the Ningi Data Protection by Design & DPIA Policy.

Where the risks to rights and freedoms of Data Subjects associated with any existing or planned Personal Data processing to be carried out by Ningi are potentially high or where otherwise required by applicable law or a supervisory authority in country or territory in which we operate, Ningi will carry out a Data Protection Impact Assessment (“DPIA”). All DPIAs are to be undertaken as set out in the Ningi Data Protection by Design & DPIA Policy. A record of DPIAs shall be kept, to include details of the outcome, the names of the parties signing off the DPIA recommendations and the date of next review.

Where a Data Controller carries out a DPIA in relation to a processing activity in which Ningi is a Data Processor, we will provide all information and assistance to the Data Controller as is reasonably required for the purpose of the DPIA.

#### **Data Subject Rights**

Data subjects have the following rights regarding Personal Data processing and the data that is collected and held about them:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (also known as the ‘right to be forgotten’);
- the right to restrict processing;

- the right to data portability;
- the right to object;
- rights with respect to automated decision-making and profiling.

Requests by Data Subjects to exercise their rights must be facilitated as set out in the Ningi Data Subject Rights Procedure.

Where Ningi is the Data Controller, we are responsible for facilitating Data Subjects' rights. Where we are a Data Processor, we must assist the Data Controller to facilitate Data Subjects' right as appropriate.

## Protection of Personal Data

All personnel must comply with the following when working with Personal Data:

- Personal Data must be handled with care at all times and must not be shared with any colleague, who does not have access to it, or with any third party without authorisation;
- physical records must not be left unattended or on view to unauthorised employees, agents, contractors or other parties at any time and must not be removed from the business premises without authorisation;
- if Personal Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- all physical copies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked filing cabinet, drawer, box or similar;
- all electronic copies of Personal Data are to be stored securely using passwords which are changed regularly, and which do not use words or phrases that can be easily guessed or otherwise compromised;
- Personal Data must not be transferred to any device personally belonging to an employee or transferred or uploaded to any personal file sharing, storage, communication or equivalent service (such as a personal cloud service);
- Personal Data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this policy and the Data Protection Law and all other applicable law (which may include demonstrating that all suitable technical and organisational measures have been taken and entering into a Data Processor contract with Ningi );
- all Personal Data stored electronically shall be backed-up regularly and securely; and
- under no circumstances must any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

In addition to the obligations set out above, all personnel involved in processing Personal Data are required to read and adhere to the Ningi Information Security Policy.

## Data Retention & Destruction

### Ningi as a Data Processor

Where Ningi is a Data Processor, we may only retain Personal Data for the duration of the data processing agreement. Upon termination of the data processing agreement, we must, at the choice of the controller, delete or return all the Personal Data to the Data Controller and delete all existing copies unless otherwise required to store a copy by UK and/or EU member state law.

#### Ningi as a Data Controller

Where Ningi is the Data Controller, we may only retain Personal Data for as long as is reasonably required and in any event, only for as long as set out in the Ningi Personal Data Retention Policy. Written authorisation from the CEO is required to retain Personal Data for longer than as set out in the Personal Data Retention Policy.

Once Personal Data records have reached the end of their life, they must be securely destroyed in a manner that ensures that they can no longer be used.

### **International Data Transfers**

We will only transfer ('transfer' includes making available remotely) Personal Data from countries in the UK/EEA to countries outside of the UK/EEA where:

- the transfer is to a country (or an international organisation) that the UK government/European Commission has determined ensures an adequate level of protection ("Adequacy");
- standard contractual clauses (or UK equivalent) adopted by the UK government/European Commission have been put in place between the entity in the UK/EEA and the entity located outside the UK/EEA;
- binding corporate rules have been implemented, where applicable; or where
- the transfer is otherwise permitted by the law.

Where Ningi is a Data Processor, transfers of Personal Data outside the UK/EEA shall only be made with the controller's agreement.

Where a transfer is not based on Adequacy, we will undertake a transfer impact assessment ("TIA") using our TIA Template to ensure that Data Subjects (whose Personal Data is transferred) continue to have a level of protection essentially equivalent to that under the UK or EU GDPR (whichever is applicable). If the TIA outcome is that the appropriate safeguard does not provide the required level of protection, we will implement supplementary measures e.g. encryption.

### **Data Breach Notifications**

All Personal Data breaches must be reported immediately to the COO and must be added to the register of Personal Data breaches.

#### Ningi as a Data Processor

Where Ningi is a Data Processor, and a Personal Data breach occurs, and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Controller must be notified immediately with further information about the breach provided as soon as information becomes available.

### Ningi as a Data Controller

Where Ningi is the Data Controller, unless a Personal Data breach occurs which is unlikely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the relevant supervisory authority must be notified of the breach without delay, and in any event, within 72 hours after having become aware of it, if this is feasible. If the notification is not made within 72 hours, it should be made as soon as possible, together with reasons for the delay. The Information Commissioner's Office (ICO) is the supervisory authority in the UK

In the event that a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of Data Subjects, all affected Data Subjects are to be informed of the breach directly and without undue delay.

Irrespective of whether Ningi is a Data Processor or a Data Controller, all data breach notifications must be handled strictly in accordance with the Ningi Personal Data Breach Procedure and be added to the Ningi Personal Data Breach Register which are located here <https://www.notion.so/ningi/GDPR-36c8befe9d9d45799c8fd3e79c8ade04?pvs=2>

### **Implementation & Policy Management**

This policy shall be deemed effective as of 03/03/2023. No part of this policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This policy will be reviewed by the COO and the Data Protection Officer annually.

## Document Control and Record Management Procedure

### **Introduction**

This procedure defines the organisation's requirements for:

- Producing, reviewing, changing, distributing, withdrawing, and destroying a Controlled Document.
- The control of Documents of external origin.
- The control of Corporate Records.

### **Applicability**

All documents required by the Information Security Management System (ISMS) shall be protected and controlled in accordance with this procedure. This includes records that need to be maintained to provide evidence of the effective operation of the ISMS.

Examples of controlled ISMS documents include:

Information Security Policy.  
Access Control Policy.  
Internal Audit Procedure.

Examples of controlled records include:

Access Control Request Forms.  
Access Control Register.  
The Continual Improvement Plan (CIP).  
Internal Audit Reports.

Company documentation outside of this scope is not subject to this procedure, however, all company, client or supplier information must be handled appropriately and in accordance with the Information Classification Policy.

All staff must understand this procedure and ensure that it is implemented whenever relevant.

## **Procedure**

All documents that fall within the scope of this procedure shall be controlled as follows:

### **Drafting a Controlled Document**

All Controlled Documents produced within the organisation shall have a documented Owner and Approver.

The Document Owner shall:

- Discuss and agree the requirements (including assessing the need for, and the purpose of the document) with the document users.
- Ensure the document conforms to the requirements which have been specified.
- Review with selected document users and the appropriate document approver before and during production and whenever changes are proposed.
- Draft the document from the latest Controlled Document template, in the relevant location within Microsoft SharePoint; such that together with reviewers' comments and details of the change history is stored correctly.
- Make edits using the Microsoft Words 'tracked changes' feature, and seek approval from the Document Owner of these edits.

Following approval:

- Name the version correctly within the Version History feature of the Microsoft Word.
- Download the final version as a PDF.
- Upload the PDF to the correct place within the Company documentation repository (MS Teams, SharePoint).
- Notify all relevant personnel of the newly created or amended document.
- Notify all other users changes.

All documents must be protected from unauthorised changes.

A Controlled Document must have at a minimum:

- A title.
- A version number showing on every page.
- A date of issue.
- A next review date.
- The name or job title of the document owner.
- The name or job title of the document approver.
- Clear confidentiality / security classification showing on every page.
- A distribution list.
- 'END OF DOCUMENT', showing on the last page of documents.

### Naming Convention

All approved Controlled Documents should have a version number included on the first page, and also be saved as a 'Named Version' in Microsoft Teams (File à Version History), using the following convention:

Tit le	Reference
v0.1	First draft of an un-issued document
v0.2	Second draft (if applicable), etc.
v1.0	First approved issue
v1.1	First draft to incorporate amendments to issue v1.0
v1.2	Second draft (if applicable), etc.
v2.0	Second approved issue

This should always correspond with the issue status recorded in the Document Register.

The ISMS Manager is responsible for ensuring that the Document Register remains up to date.

### Layout of the ISMS Documentation

When creating a Company ISMS policy, process or procedure, the following template should be used:

Ningi\_ISMS\_TEMPLATE.

Refer to the Document Register to obtain the latest version of the template.

If in doubt, ask the ISMS Manager.

### Change Control for ISMS Documentation

Unless otherwise specified within the document, all changes to ISMS Controlled Documents will result in a re-issue to the next issue version level.

The Document Owner shall:

- Make all edits in the original document using the 'tracked changes' mode.
- Get approval for these edits from the Document Approver, if required.
- Amend the document control section at the beginning of the document, and name the current version.

- Ensure that the final, approved version of the document is correctly published to the appropriate repository.
- Advise the ISMS Manager to update the Document Register with the new version number; and,
- Notify the relevant parties that a new version has been published.

If in doubt, the Document Owner should refer any query to the ISMS Manager.

### **Distribution to Third Parties**

ISMS Documentation may not be distributed to a third party unless explicitly permitted by the Managing Director and only if a Non-Disclosure Agreement with the third party is in place.

Documentation relating to client bids and client, or internal Company projects may only be distributed to sub-contractors, partners or other collaborators who have signed a Non-Disclosure Agreement and with prior email approval from a Managing Director.

The Document Owner is responsible for the secure distribution of Draft and Issued Controlled Documents. When issuing new versions, the changes must be identified in the Document Control table.

### **Storage**

Controlled Documents and Records shall be stored in such a way to prevent damage, deterioration, unauthorised changes or loss. Records will be stored digitally on the Company approved repository.

Electronic copies of all documents and records that are generated by the Company and form the corporate record of Company operations shall be held in the approved Company repository. Access should be restricted.

Note: A controlled document that is printed or saved outside the dedicated folders is no longer considered controlled.

### **Withdrawal and Archive**

The Document Owner is responsible for notifying relevant personnel when a Controlled Document has been identified as obsolete and to be withdrawn from use, ensuring that superseded copies of the documents are archived to prevent inadvertent use.

### **Disposal**

At the end of the agreed retention period, the Document Owner will review the need for disposal and agree appropriate action. This will include consideration of the requirement for 'shredding' or other appropriate secure disposal of hard copies of documents or records which may be of a confidential nature.

### **Information Deletion**

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements, information stored in information systems, devices or in any other storage media should be deleted when no longer required.

When deleting information, Ningi will:

Select a deletion method (i.e., electronic overwriting, cryptographic erasure).

Record the results of deletion as evidence.

When using suppliers of information deletion services, obtain evidence of the information deletion from

them.

### Documents of External Origin

Documents of External Origin, e.g. copies of ISO Standards, maintenance manuals or application handbooks, may be subject to changes when updates are issued by the manufacturer or other external body. Documents of this type also need to be controlled.

A copy of any such documents must be sent to the ISMS Manager, who will place them on file and assigned a document reference number. The document reference number is then recorded on the Document Register.

### Control of Records

Company records that need to be maintained to provide evidence of the effective operation of the ISMS shall be managed in accordance with this procedure.

All ISMS records shall:

Clearly identify the date and place the work was carried out and the identity of the person who carried out the work.

Be stored safely and in such way as to be easily retrievable.

Be uniquely identifiable, and the place of storage logged as defined in the relevant Company procedure.

### Information Control

The organisation's Information Classification Policy also identifies the requirements for the classification, handling, and storage of information and associated best practice.

### Retention

Document retention is increasingly important to comply with statutory minimum requirements and in relation to any litigation that may arise either in respect of clients, suppliers or employees. Premature destruction of important documents can materially prejudice a case.

The following table details the documents to be kept and the length of time they should be retained. The retention periods are based on generally accepted best practice and where applicable UK law. At a minimum, the retention periods set out below should apply.

Title	Reference
ISMS Policies, Procedures, Forms & Templates	3 years
Continual Improvement Plan	3 years from last date
Audit Reports	3 years
Incident Logs	3 years from last recorded incident
IS Risk Assessments	3 years
Business Continuity Plans and Tests	3 years
Visitors Logbook	3 years
Documents of External Origin	6 years



Staff Training and Competence Records	6 years after employment ceases
Supplier and Customer Contracts (including variations)	6 years after completion or termination of contract

### **Compliance and Monitoring**

Compliance with this and all other policies and procedures is mandatory.

Any breach of policy may result in disciplinary action, up to and including dismissal.

### **Monitoring**

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

### **Audit and Review**

#### **Internal Review**

Compliance with this policy will be monitored through Information Security Internal Audits, and by other management checks as required.

#### **External Review**

Inspections by external auditors may be carried out from time to time.

As part of these activities, external inspectors may ask to view internal records. Supervised access to such records must be provided where requested.

Copies of records must not be removed from site by an inspector unless this has been specifically approved by the ISMS Manager.

### **Policy Review**

This policy will be reviewed by the ISMS Manager or his nominated delegate at regular intervals, not exceeding 1 year, or when business changes warrant it as part of the continual improvement process.

## **Information Classification Policy**

### **Introduction**

The purpose of this policy is to ensure that all information and data generated, accessed or stored by Ningi is suitably classified according to defined criteria.

Information is a critical asset. Ningi's information is used to create know-how used to deliver our services, support customers and to win new business. The information we hold includes data shared with us by clients and employees to whom we owe contractual obligations and personal data in respect of which we have legal obligations.

It is therefore necessary to implement a classification scheme that determines how our information must be protected and who shall be allowed to access to it.

### **Applicability**

This policy applies to all staff, including employees, contractors and interns working for or under the control

of Ningi.

### **Scope**

This policy relates to all information and data generated, accessed, modified, transmitted or stored by Ningi, including information provided to us by staff, partners, clients and potential clients. This includes electronic information and information held in paper or other physical records.

### **Policy**

All information and data generated, accessed, modified, transmitted or stored by Ningi must be proactively classified into one of the following four categories:

- Public.
- Internal / Internal Use Only.
- Confidential; and.
- Client Confidential.

Further information on each of these classifications, together with examples, are provided below. Examples are illustrative only, unless otherwise stated.

When classifying information, employees must consider the value and criticality of the information to Ningi and the likely impact to Ningi, its staff, partners and clients if the information is disclosed to or modified by an unauthorised party. It is important to specifically consider whether the information:

- Has been made available to us by a client or other third party under an expectation or obligation of confidentiality.
- Includes or might include the personal data of any individual, including Ningi or client employees.
- Contains any Ningi proprietary information, data, knowledge or other Intellectual Property (IP).

Document classification must be clearly displayed in Document Control tables and repeated in the footer of each page of a document.

### **“Public” Classification**

#### **Description**

“Public” classification should be applied to information which is or can be disclosed to the public without limitation using established publication methods and without implication for Ningi.

#### **Distribution and Transfer**

There is no requirement to label documentation labelled “Public”. Non-labelled documentation is considered “Public” by default.

There are no restrictions on methods of communicating Public information.

#### **Examples**

By way of illustration only, some examples of Public information include:

- Information on the Ningi website.
- Information that is widely available in the public domain.

Marketing collateral shared with partners, clients and potential clients.

Other information widely available in the public domain.

### **“Internal” Classification**

#### **Description**

“Internal” or “Internal Use Only” or “Internal Only” classification should be applied to information which is not published freely by Ningi because it adds value to the organisation or is relatively private in nature, but which should be accessible by all employees and workers.

#### **Distribution and Transfer**

Internal information may be disclosed and disseminated within Ningi but must not be disclosed to third parties without authorisation from a member of the exec team/Senior Management Team.

There are no restrictions on methods of communicating Internal information.

#### **Examples**

By way of illustration only, some examples of Internal information include:

Employee names and work contact details.

Internal policies, procedures and guidelines.

Know-how used to process client information.

Standard operating procedures, including business continuity plans and risk assessments.

Internal management communications.

### **“Confidential” Classification**

#### **Description**

“Confidential” classification should be applied to information which has significant value to Ningi.

Unauthorised access to or disclosure of Confidential Information could lead to financial or reputational damage to Ningi so processing, access, storage and transmission must be secured.

#### **Distribution and Transfer**

Confidential information shall only be made available to Ningi employees on a need-to-know basis, where the information is necessary for the performance of their duties and who are under a contractual obligation of confidentiality.

Confidential information may not be disclosed to third parties without authorisation from a member of the Executive Team unless an NDA is in place. This includes granting access to systems that store or process Confidential information. Confidential information must be protected against unauthorised access or disclosure and to prevent loss or theft.

Paper copies of Confidential information and portable electronic storage media holding Confidential information must be secured in locked storage (such as a filing cabinet or drawer) when not in use.

Confidential information shall only be communicated electronically using the following methods:

Secure file transfer methods approved by management; or

Emails which are fully encrypted or to which Ningi Confidential information has been attached as an encrypted attachment using encryption methods approved by management.

In any event, passwords used to protect Confidential information during communication or electronic transmission must meet the passwords standards set out in the Ningi Password Management Policy. Passwords must not be shared in the same message as Confidential Information.

### **Examples**

By way of illustration only, some examples of Confidential information include:

- Personal data (such as employee HR records).
- Company financial information and reports.
- Confidential customer business data and confidential contractual documents.
- Ningi business plans.
- Engineering files, designs, source code, and other company IP.
- Internal management information.

### **“Client Confidential” Classification**

#### **Description**

Client Confidential information (“CCI”) is information that Ningi receives from clients. CCI may include personal data about customer employees to which data protection laws will apply.

Where it is not possible to apply classification to an electronic CCI document, the digital folder in which they are stored should be clearly labelled.

#### **Distribution and Transfer**

Unauthorised access or disclosure of Customer Confidential information could lead to financial or reputational damage to Ningi and to affected clients, so processing, access, storage and transmission must be secured.

CCI shall only be made available to Ningi employees under an obligation of confidentiality who require access to it to provide services to the client. Access to systems that process or store CCI shall be restricted in line with the principle of least privilege.

Paper copies of CCI and portable electronic storage media holding CCI must be secured in a lockable container (such as a filing cabinet or drawer) when not in use.

CCI must not be disclosed to a third party unless specifically requested in writing by a client and authorised by a member of the executive team. Where disclosure has been approved, secure transmission methods must be used as required for Confidential information.

### **Examples**

By way of illustration only, some examples of Client Confidential information include:

- Information collected from clients during requirement gathering and commercial meetings.
- End user client data
- Statements of Work (SoW), client contracts.

### **Retention and Destruction**

## **Retention**

Personal data shall be retained for no longer than is set out in Ningi's Document Control and Records Management Procedure.

Client Confidential information shall be retained for 6 months following the completion of the specific projects or engagement with the client to which the CCI applies, unless otherwise agreed in writing with the client or required by the contract between Ningi and the client. Client contracts and related documents may be kept indefinitely to maintain and evidence good record keeping.

Information shall be securely destroyed as set out in the Ningi Information Security Policy and Media Handling and Disposal Policy.

## **Information Deletion**

Ningi's policy is for information to be deleted when it is no longer required. Detail on this process can be found in the Ningi Document Control and Records Management Procedure.

## **Sharing Information Externally**

As well as following instructions for the correct methods of sharing information externally as outlined in this policy, special care must be taken not to inadvertently share information externally that is not already public. This could include:

- Copying and pasting text into any unapproved third-party proofreading, translation or AI tool such as ChatGPT.

- Using a browser extension that has not been approved by the CTO, which can read the contents of your screen.

- The use of software that is in breach of the Acceptable Use Policy.

Remember that entering information that isn't already public into a tool such as the above amounts to external sharing and is in breach of this policy. Special care must be taken not to do so.

## **Compliance and Monitoring**

- Compliance with this and all other policies and procedures is mandatory.

- Any breach of policy may result in disciplinary action, up to and including dismissal.

## **Monitoring**

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

## **Audit and Review**

### **Internal Review**

Compliance with this policy will be monitored through Information Security Internal Audits, and by other management checks as required.

### **External Review**

Inspections by external auditors may be carried out from time to time.

As part of these activities, external inspectors may ask to view internal records. Supervised access to such records must be provided where requested.

Copies of records must not be removed from site by an inspector unless this has been specifically approved by the ISMS Manager.

**Policy Review**

This policy will be reviewed by the ISMS Manager or his nominated delegate at regular intervals, not exceeding 1 year, or when business changes warrant it as part of the continual improvement process.

## Information Security Policy

**Introduction**

This policy documents Ningi's commitment to information security, continual improvement and satisfying applicable information security requirements of its interested parties such as employees, clients, partners and suppliers.

### **Applicability**

This policy applies to all staff, including employees, contractors and interns working for or under the control of Ningi.

### **Information Security Statement**

“Ningi recognises that the security of the information entrusted to us by our employees, customers, partners and suppliers is of paramount importance, and ensures the confidentiality, integrity and availability of that information through Policies, Processes and Controls to provide our stakeholders with the assurance that their information is in safe hands”.

### **Policy**

#### **Principles**

Ningi is committed to the development, implementation and maintenance of an Information Security Management System (ISMS) that:

- Provides assurance within Ningi and to our clients, partners and suppliers that the availability, integrity and confidentiality of their information will be maintained appropriately;
- Manages information security risks to all Ningi and customer assets;
- Protects the Ningi’s ongoing ability to meet contracted commitments through appropriate Business Continuity;
- Bases information security decisions and investments on the risk assessment of relevant assets considering Integrity, Availability and Confidentiality;
- Considers business and legal or regulatory requirements and contractual security obligations;
- Maintains awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities;
- Minimises the business impact and deals effectively with security incidents;
- Meets the requirements of any other interested parties not already specified.

#### **The Policy in Operation**

This policy is supported by the following objectives:

- A senior management team that supports the continuous review and improvement of the Information Security Management policies and processes;
- Implementation of company-wide policies and procedures that support our Information Security Statement;
- General policies and processes for the protection of corporate information as well as employee, client and supplier information;
- Implementation of an Information Security Risk Assessment Process that assesses the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities and controls currently in place;
- Development and implementation of a Business Continuity Plan to counteract disruptions to business activities and to protect critical business processes from the effects of major failures or disasters;
- Defined physical and logical access controls to prevent unauthorised access, damage to and interference with business premises and information;
- Implementation of incident management and escalation procedures for reporting and investigating

security incidents for review and action.

All information security policies and procedures can be found within Ningi's Information Security Management System (ISMS). It is the responsibility of employees and contractors to read these and report any non-compliance in accordance with the Information Security Incident Management Process.

### **Roles, Responsibilities and Authorities**

#### **The Management Team Ensures:**

- An Information Security Policy and supporting processes are set and maintained;
- The review and monitoring of security incidents;
- Changes to Ningi's organisation and operations are reviewed to assess the impact on information security;
- The promotion of security requirements and issues throughout Ningi;
- A continual improvement programme is maintained for Ningi's information security arrangements.

#### **The Managing Director:**

- Actively supports information security within the organisation through clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities;
- Provides the resources needed to maintain the ISMS and support information security related activities;
- Approves the assignment of specific roles and responsibilities for information security across the organisation.

#### **The ISMS Manager, Supported by the Management Team:**

- Coordinates Information Security related activities within the organisation;
- Schedules, chairs and documents Information Security Management Reviews;
- Reviews and approves information security policies, methods and processes;
- Maintains information security related policies and procedures, including annual reviews to ensure continuing suitability, adequacy and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the information security policies and processes;
- Maintains change, control and integrity of information security documents;
- Analyses incident reports, identifies root causes and planned improvement actions and reports to the Directors, recommending actions where appropriate;
- Conducts risk assessments of information security assets, identifying significant threat changes and exposure of information and information processing facilities to threat;
- Organises and conducts audits and reviews of the information security policies and processes;
- Periodically reviews the organisation's business continuity requirements and maintains the company's Business Continuity Plan;
- Manages the external assessment interface for ISO 27001 certification;
- Ensures that Directors and staff are fully aware of their obligations with respect to information security;
- Delivers information security induction to new starters, and periodic refresher training to existing staff.

#### **Staff**

All Ningi staff, permanent and contractors, are responsible for ensuring Ningi policies and associated requirements are complied with, within their area of responsibility and operation.



## **Continual Improvement**

Ningi is committed to a process of continually improving the effectiveness of its ISMS.

To this end, a Continual Improvement Plan (CIP) is operated and maintained.

The ISMS Manager in conjunction with the ISMS Management Team is responsible for ensuring that all quality and information security related improvement plans, corrective actions and non-conformities are collated in the CIP. These may arise from several sources, including:

- Management reviews;
- Internal and external audits;
- Annual business improvement objectives;
- Incident reporting;
- Change management;
- Financial reporting;
- Resourcing reporting;
- Business continuity testing;
- Suggestions and issues raised by employees;
- Client complaints and compliments;
- Supplier reviews;
- Other Ningi reviews and meetings;
- Day to day business activities.

## **Data Protection**

Ningi takes Data Protection compliance seriously and places a high importance on protecting the Personal Data of individuals with whom we work including our clients, end customers and employees. We are committed to the fair, lawful and transparent handling of Personal Data and to facilitating the rights of individuals.

We have appointed an external DPO in line with Article 38 of UK GDPR, the contact details for which are as follows.

Evalian Ltd  
West Lodge  
Leylands Business Park  
Colden Common  
Hampshire  
SO21 1TH  
United Kingdom

Email: [DPO@evalian.co.uk](mailto:DPO@evalian.co.uk)

Phone: +44 (0)333 050 0111

Website: [www.evalian.co.uk](http://www.evalian.co.uk)

Ningi is registered as a Data Controller with the Information Commissioner's Office having registration number ZB098889.

## Organisational Measures

We have implemented the following procedures to support data protection compliance:

- Data Protection Policy
- Data Subjects Rights (DSRs) Procedure
- Personal Data Breach Procedure
- Data Protection Impact Assessments (DPIAs) Procedure
- Data Protection by Design and Default Policy
- Personal Data Retention Policy and Deletion Schedule
- Register for DSRs, Personal Data Breaches and DPIAs
- Record of Processing Activities (RoPA)
- Risk Register
- Employee training and training tracker

## Third Party Processors

Where third-party processors are used, we carry out the relevant due diligence checks with these organisations, to ensure they will process the personal data involved to the required standard and implement appropriate security measures.

UK GDPR compliance Data Processing Agreements are in place where we use third party processors.

## International Transfers

We will only transfer ('transfer' includes making available remotely) Personal Data from countries in the UK/EEA to countries outside of the UK/EEA where:

- the transfer is to a country (or an international organisation) that the UK government/European Commission has determined ensures an adequate level of protection ("Adequacy");
- standard contractual clauses (or UK equivalent) adopted by the UK government/European Commission have been put in place between the entity in the UK/EEA and the entity located outside the UK/EEA;
- binding corporate rules have been implemented, where applicable; or where the transfer is otherwise permitted by the law.

Where Ningi is a Data Processor, transfers of Personal Data outside the UK/EEA shall only be made with the controller's agreement.

## Insurance Confirmation



Stuart House, St Johns Street, Peterborough, PE1 5DD

Direct tel 01733 294500  
Office 01733 563957  
Mobile 01733 295295

denise.gorman@marshcommercial.co.uk  
www.marshcommercial.co.uk

16th April 2025

**To Whom It May Concern**

**CONFIRMATION OF INSURANCE: Ningi Limited**

As requested by the above client, we are writing to confirm that we act as Insurance Brokers to the client and that we have arranged insurance(s) on its behalf as detailed below:

**PUBLIC, PRODUCTS & EMPLOYERS LIABILITY**

<b>POLICYHOLDER :</b>	Ningi Limited		
<b>BUSINESS DESCRIPTION :</b>	Software provider for the financial advice industry. Act as a processor of data for a multitude of advice firms, providing software to increase efficiencies and innovation.		
<b>INSURER :</b>	Royal & Sun Alliance Insurance Ltd		
<b>POLICY NO :</b>	RSAP3043141300		
<b>PERIOD OF COVER :</b>	21st April 2025	to :	20th April 2026
<b>LIMIT OF INDEMNITY :</b>	Public Liability - any one event		£10,000,000
	Products Liability - period of insurance		£10,000,000
	Employers Liability - any one occurrence		£10,000,000
<b>EXCESS:</b>	£0.00 - Public Liability		

**PROFESSIONAL INDEMNITY**

<b>POLICYHOLDER :</b>	Ningi Limited		
<b>BUSINESS DESCRIPTION :</b>	Software provider for the financial advice industry. Act as a processor of data for a multitude of advice firms, providing software to increase efficiencies and innovation.		
<b>INSURER :</b>	Royal & Sun Alliance Insurance Ltd		
<b>POLICY NO :</b>	RSAP3043141300		
<b>PERIOD OF COVER :</b>	21st April 2025	to :	20th April 2026
<b>LIMIT OF INDEMNITY :</b>	Any one occurrence		£5,000,000
<b>EXCESS:</b>	£1,000		

We have placed the insurance which is the subject of this letter after consultation with the client and based upon the client's instructions only. Terms of coverage, including limits and deductibles, are based upon information furnished to us by the client, which information we have not independently verified.

This letter is issued as a matter of information only and confers no right upon you other than those provided by the policy. This letter does not amend, extend or alter the coverage afforded by the policies described herein. Notwithstanding any requirement, term or condition of any contract or other document with respect to which this letter may be issued or pertain, the insurance afforded by the policy (policies) described herein is subject to all terms, conditions, limitations, exclusions and cancellation provisions and may also be subject to warranties. Limits shown may have been reduced by paid claims.

We express no view and assume no liability with respect to the solvency or future ability to pay of any of the insurance companies which have issued the insurance(s).

We assume no obligation to advise yourselves of any developments regarding the insurance(s) subsequent to the date hereof. This letter is given on the condition that you forever waive any liability

Marsh Commercial is a trading name of Marsh Ltd. Marsh Ltd is authorised and regulated by the Financial Conduct Authority for General Insurance Distribution and Credit Broking (Firm Reference No. 307511). Copyright © 2021 Marsh Ltd. Registered in England and Wales Number: 1507274. Registered office: 1 Tower Place West, Tower Place, London EC3R 5BU. All rights reserved.



## List of Sub-processors

Key:

App: ●

CRM/Back-office: ●

AI Suite: ●

Engage: ○

This is a list of sub-processors we use throughout Ningi and we have indicated which part of our tech uses each sub-processor.

The Controller has authorised the following sub processors:

Name	Google LLC ●
Contact person's name, position and contact details	Data Privacy Team <a href="https://firebase.google.com/support?category=other-category&amp;urgency=account&amp;summary=%5BPRIVACY%5D%20">https://firebase.google.com/support?category=other-category&amp;urgency=account&amp;summary=%5BPRIVACY%5D%20</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Data storage provider which may be required to provide technical support in the event of issues with its storage.

Name	Heroku ● ● ●
Contact person's name, position and contact details	Data Privacy Team <a href="mailto:security@salesforce.com">security@salesforce.com</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Cloud application platform provider which may be required to provide technical support in the event of issues with its storage.

Name	MongoDB Atlas ● ● ●
Contact person's name, position and contact details	Data Privacy Team +44 203 903 0584
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Multi-Cloud application data platform provider which may be required to provide technical support in the event of issues with its storage.

Name	Sign Request ●
Contact person's name, position and contact details	Please contact <a href="mailto:support@signrequest.com">support@signrequest.com</a> SignRequest B.V., Singel 542,1017 AZ Amsterdam, The Netherlands, +31 (0) 20894 36 57
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	E-signature services for client onboarding and document signing.

Name	Hotjar ● ○
Contact person's name, position and contact details	Hotjar Ltd, Dragonara Business Centre, 5th Floor, Dragonara Road,, Paceville St Julian's STJ 3141, Malta. Telephone number: +1 (855) 464-6788
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Product experience insight tool for behavioural analytics and feedback from users.

processors are authorised)	
----------------------------	--

Name	Unami ●
Contact person's name, position and contact details	Data Privacy Team <a href="mailto:privacy@umami.is">privacy@umami.is</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Provider of website analytics and feedback data

Name	Intercom ○
Contact person's name, position and contact details	Data Privacy Security Team <a href="https://www.intercom.com/security">https://www.intercom.com/security</a> .
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Automated customer service communication tool


Name	Smart Search ●
Contact person's name, position and contact details	Business Development <a href="mailto:Michael.Shaw@smartsearch.com">Michael.Shaw@smartsearch.com</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Anti-money laundering tool


Name	eValue ●
Contact person's name, position and contact details	Inside Sales Executive <a href="mailto:siobhan.williams@ev.uk">siobhan.williams@ev.uk</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Attitude to risk profiling tool

Name	Mailgun ● ○
Contact person's name, position and contact details	Data Privacy Team <a href="mailto:privacy@mailgun.com">privacy@mailgun.com</a> .
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	API tool for automated transactional emails

Name	Recall ●
------	----------

Contact person's name, position and contact details	Data Privacy Team <a href="mailto:hello@recall.ai">hello@recall.ai</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	API tool for AI transcription

Name	Vercel 
Contact person's name, position and contact details	Data Privacy Team <a href="mailto:Privacy@vercel.com">Privacy@vercel.com</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Vercel simplifies web development with automated deployments and a global edge network. Its serverless architecture offers seamless scaling for modern applications, supporting both frontend and server-side processing, including APIs

Name	Assembly AI 
Contact person's name, position and contact details	Data Protection Officer <a href="mailto:legal@assemblyai.com">legal@assemblyai.com</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Third party used for speech to text generation.

Name	AWS S3 
Contact person's name, position and contact details	Data Protection Officer <a href="mailto:Aws-eu-privacy@amazon.com">Aws-eu-privacy@amazon.com</a>
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Amazon S3 (Simple Storage Service) is a cloud-based object storage service offered by Amazon Web Services (AWS).

## Media Handling and Disposal Policy

### Introduction

The purpose of this policy is to set out the controls that must be in place when using and handling media. It is intended to mitigate the following risks:

- ✓ Loss or theft of media, including of the data saved on them;
- ✓ Compromise of confidential information through observation by unauthorised persons;

- ✓ Introduction of viruses and malware on the network;
- ✓ Loss of reputation.

## Applicability

This policy applies to all staff, including employees, contractors and interns working for or under the control of Ningi.

## Policy

To protect information, Ningi staff and contractors must safeguard archive media against disclosure, theft or damage.

Appropriate media labelling, storage, transport and disposal are risk mitigation controls.

Media includes items such as:

- ✓ All removable digital storage devices, including USB drives, smart phones, etc.;
- ✓ CDs and DVDs;
- ✓ Paper;
- ✓ Data or information that is stored locally on mobile devices.

It is important that the controls set out in this policy are observed at all times in the use and transportation of media.

## The Policy in Operation

### Use of Media

The following sections describe how to handle different media types and events in the media lifecycle. When in doubt about the information stored on media, label, log and store media securely.

- ✓ Regardless of method, the handling, processing, transmission and/or storage of Ningi information should be implemented through means that limit the potential for unauthorised disclosure;
- ✓ Archive material should be labelled to ensure information can be logged, tracked, easily retrieved if required, and effectively protected;
- ✓ In the event that files containing information classified as Confidential or Internal Use Only need to be saved to removable media, the removable media must be encrypted and registered as a Ningi approved information asset;
- ✓ Employees, whilst travelling or working away from the office, should ensure that Ningi information is adequately safeguarded from unauthorised access and viewing. This applies regardless of whether the information is in paper form, recorded on CDs, DVDs or other electronic or digital media. The use of a screen filter applied to laptop screens is recommended;
- ✓ The Mobile Devices Policy will be followed when utilising laptops and other portable devices such as smartphones and tablets;
- ✓ Ningi information may be sent via local postal service or a commercial delivery service. Where possible, mail must be packaged in a way that does not disclose its contents;
- ✓ During non-office hours, Ningi information and removable electronic media containing Ningi information must be secured within a locked office or a locked container;
- ✓ Custodians of all personally identifiable information must ensure that it is secured when not in use;
- ✓ You must not travel internationally with any media, computers or mobile devices that contain information that is subject to export control, without prior approval from the COO or CTO.

## **Disposal of Media (End of Life)**

The following procedures must be followed when disposing of records and equipment:

- ✓ Before disposal, required material should be backed up off hard disks, DVDs, USB sticks and other media;
- ✓ Any device that can store data must be handed over to the CTO for disposal;
- ✓ All electronic equipment must be disposed of in accordance with WEEE regulations. Return such equipment to the CTO who will take the necessary steps to ensure that it is disposed of appropriately;
- ✓ Any confidential paper documentation should be cross-shredded before disposal.

## **Compliance and Monitoring**

- ✓ Compliance with this and all other policies and procedures is mandatory;
- ✓ Any breach of policy may result in disciplinary action, up to and including dismissal.

### **Monitoring**

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

### **Audit and Review**

#### **Internal Review**

Compliance with this policy will be monitored through Information Security Internal Audits, and by other management checks as required.

#### **External Review**

Inspections by external auditors may be carried out from time to time.

As part of these activities, external inspectors may ask to view internal records. Supervised access to such records must be provided where requested.

Copies of records must not be removed from site by an inspector unless this has been specifically approved by the ISMS Manager.

#### **Policy Review**

This policy will be reviewed by the ISMS Manager or his nominated delegate at regular intervals, not exceeding 1 year, or when business changes warrant it as part of the continual improvement process.



# Mobile Device Policy

## Introduction

The purpose of this policy is to set out the controls that must be in place when using mobile devices. It is intended to mitigate the following risks:

- ✓ Loss or theft of mobile devices, including the data on them;
- ✓ Compromise of classified information through observation by non-authorised people;
- ✓ Copyright – software copied onto a mobile device could violate licence
- ✓ Introduction of viruses and malware to the Ningi systems;
- ✓ Loss of reputation;
- ✓ Non-Compliance with various identity theft and privacy laws

It is important that the controls set out in this policy are observed at all times in the use and transportation of mobile devices.

## Applicability

This policy applies to all staff, including employees, contractors and interns working for or under the control of Ningi.

## Policy Statement

Ningi recognises that staff need to work in a mobile manner, across multiple devices, and locations.

Ningi enables staff to access its systems and folders through company-issued devices, from any location, via our secure remote desktop services.

Ningi issues corporate devices to staff where this is a requirement of their role. This policy sets out how Ningi manages such mobile devices and provides guidance for workers on their use.

Personally owned devices may not be connected, synchronised with or otherwise used to conduct Ningi business except as set out in the Ningi BYOD Policy.

Ningi allows the use of personally owned devices to conduct Ningi business, as long as these are registered as BYOD devices. Devices must be registered in our Mobile Device Management solution Kandji, and both Ningi-provided and BYOD devices will be logged in our company device register.

Laptops, Notebooks, and hybrid devices

- ✓ Smartphones and tablets

## Conditions of Use

As a user of an Ningi-supplied mobile device, you agree to comply with the conditions of use detailed below.

## Physical Protection

You must ensure that laptop computers are protected when transported to reduce the risks from environment threats and hazards;

You must ensure that mobile devices are stored securely when not in use to prevent unauthorised access;

You must ensure that all sessions are logged off and that laptops are shutdown (not left in sleep/hibernation mode) when in transit;

You must not leave mobile devices unattended in public view, such as in the back of a car or in a meeting room or hotel lobby. The use of a laptop lock should be considered;

You must not remove any identifying marks on mobile devices such as a company asset tag or serial number;

You must log any faults with the device with the CTO;

You must not add peripheral hardware to a company mobile device without the approval of the CTO.

#### ▪ **Access Control**

For smartphones, you must use biometric security or a PIN code which is at least 6 digits long;

You must not keep access tokens, Personal Identification Numbers or other security items with the devices, unless they are protected by a company approved password management vault;

You must ensure that the device screen locks after a short period of not being used and requires a biometric scan, an access code or password to unlock it;

You must use a password of the strength that is enforced by the system that is being accessed. Passwords should be difficult to guess (refer to the Password Management Policy for guidance);

You must return the device to the CTO or nominated delegate at any time for problem resolution and maintenance purposes, or inspection and audit if this is required;

You must not install any unauthorised software on the device without consulting the CTO;

You must not change the configuration or setup of the device without consulting the CTO;

Users with privileged access rights to business-critical systems will have Multi-Factor Authentication (MFA) applied to their devices for additional security.

#### ▪ **Cryptographic Techniques**

Laptops and smartphones must be encrypted;

Staff will not be able to disable the encryption feature.

#### ▪ **Backups**

Files must be saved to Microsoft SharePoint online or your Microsoft Teams storage from where they can be accessed from your mobile device. Files must never be saved locally to mobile devices.

Refer to the Backup and Restore Policy for additional information.

#### **Virus Protection**

Virus protection is installed on laptops as part of the standard build;

Virus protection must not be disabled under any circumstance, unless expressly authorised by the CTO; and then only for the minimum time required for the purpose for which protection must be disabled.

## Overlooking

When in public places, ensure that you site the device such as unauthorised people cannot view and potentially take photographs or videos of the screen;

The use of screen filters is recommended.

## Compliance and Monitoring

- ✓ Compliance with this and all other policies and procedures is mandatory;
- ✓ Any breach of policy may result in disciplinary action, up to and including dismissal.

## Monitoring

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

## Audit and Review

### Internal Review

Compliance with this policy will be monitored through Information Security Internal Audits, and by other management checks as required.

### External Review

Inspections by external auditors may be carried out from time to time.

As part of these activities, external inspectors may ask to view internal records. Supervised access to such records must be provided where requested.

Copies of records must not be removed from site by an inspector unless this has been specifically approved by the ISMS Manager.

## Policy Review

This policy will be reviewed by the ISMS Manager or his nominated delegate at regular intervals, not exceeding 1 year, or when business changes warrant it as part of the continual improvement process.

# Password Policy

## Machine passwords

Description	Value	Managed by
Minimum passcode length	12	Kandji
Minimum complex characters	1	Kandji
Maximum passcode age	365 days	Kandji
Require Passcode After Sleep or Screen Saver Begins	Immediately no grace period	Kandji
Start Screen Saver After	5 Minutes	Kandji

Maximum Failed Attempts Before Account Lockout	10	Kandji
Account Lockout Duration	5 Minutes	Kandji

### External services passwords

Passwords should be managed and generated via 1Password. This is to ensure their complexity and random selection. Passwords should not be made up without the use of 1Password. Passwords should be reset if a breach has possibly been made.

## Personal Data Breach Procedure

### Introduction

This Personal Data Breach Procedure (this “procedure”) sets the procedure to be followed by all employees, workers and contractors (“personnel”, “you”, “your”) of Ningi (“Ningi”, “we”, “us”, “our”) in the event of a Personal Data breach.

This procedure has been prepared with due regard to the data protection laws applicable to Ningi and our Personal Data processing activities. These data protection laws include the UK GDPR and/or the EU GDPR (whichever is applicable) and DPA 2018, (collectively referred to throughout this procedure as the “Data Protection Law”).

This policy should be read together with the following related documents:

- Ningi Data Protection Policy
- Ningi Data Breach Assessment Form
- Ningi Personal Data Breach Register

**Please note, that the definitions for any undefined terms in this procedure can be found in clause 4.1 of Ningi’s Data Protection Policy and are applicable to this procedure.**

## **Purpose of this Procedure**

When processing Personal Data, Ningi may be required by Data Protection Law to notify other parties following a data breach affecting Personal Data. A Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

When processing as a Data Controller, Data Protection Law requires that:

- unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of Data Subjects affected in the UK and/or the EEA it must be reported to the relevant supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it; and
- any Personal Data breach likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of Data Subjects affected in the UK and/or the EEA must be reported to the affected Data Subjects without undue delay except where specific conditions are met.

When processing as a Data Processor, the Data Protection Law requires Ningi to notify the Data Controller without undue delay following a data breach affecting their Personal Data.

It is important to meet these obligations to ensure we comply with Data Protection Law and to ensure we respect the rights and freedoms of Data Subjects. The purpose of this procedure is to set out what is required of Ningi following a data breach and the steps to be taken in such event.

This procedure applies to all Ningi personnel. You must follow this procedure when responding to a Personal Data breach. Any failure to do so may result in disciplinary action.

## **Scope**

This policy applies to all Personal Data processed by Ningi , whether held in electronic form or in physical records, and regardless of the media on which that Personal Data is stored. It applies to Personal Data we process as a Data Controller and Personal Data we process as a Data Processor (on behalf of our customers).

Ningi is registered as a Data Controller with the Information Commissioner's Office ("ICO") having registration number ZB098889.

## **Steps to Follow**

In the event of a Personal Data breach, the following steps must be followed:

### Always

No.	Step	Action
1.	A potential Personal Data breach is identified.	<p>All potential Personal Data breaches must be reported urgently to <a href="mailto:dataprotection@ningi.co.uk">dataprotection@ningi.co.uk</a>, as well as informing the Head of Performance. The report must set out all details relating to or known about the potential breach.</p> <p>This report should clearly set out whether it is believed to be a potential breach including whether it is still under investigation or whether a definitive breach has taken place.</p> <p><b>A potential breach should be referred to as an ‘incident’ as opposed to a ‘breach’ until it has been established that a breach has actually occurred.</b></p>
2.	Investigate whether a Personal Data breach has occurred.	Ningi shall immediately undertake an initial investigation as set out at <i>Section 5</i> to establish whether a breach has occurred.

### Ningi as a Processor

3.	Notify the Data Controller where Ningi is a Data Processor.	If the investigation establishes a breach has occurred which affects Personal Data processed by Ningi, the Data Controller (our customer) shall be notified without undue delay or in the timescale agreed with the relevant Data Controller as set out at <i>Section 8</i> of this procedure.
----	---	--

### Ningi as a Data Controller

4	Assess the risks to affected Data Subjects.	The initial investigation shall include an assessment of the risks to rights and freedoms of Data Subjects in accordance with Appendix 1 of this procedure.
5	Notify the ICO/relevant supervisory authority where required.	If it is determined that the breach is likely to result in a risk to Data Subjects, the ICO/relevant supervisory authority shall be notified without undue delay in the manner set out at <i>Section 6</i> of this procedure.
6	Notify affected Data Subjects where required.	If it is determined that the breach is likely to result in a high risk to Data Subjects the affected Data Subjects shall be notified without undue delay as set out at <i>Section 7</i> of this procedure.
7	Record the Personal Data breach and details of the actions taken.	A record of all Personal Data breaches must be kept, using the Ningi Personal Data Breach Register to demonstrate accountability and compliance with Data Protection Law.

### Initial Investigation

Upon first being informed of, or upon first identifying a potential Personal Data breach, Ningi shall immediately undertake a short period of initial investigation. The investigation shall be led by the Head of Performance or their designate, supported by such other persons as they shall deem necessary.

The Ningi Data Protection Officer (“DPO”) shall be kept informed as to the progress and findings of the investigation at all times, and shall advise on the steps to be taken to ensure compliance with our legal obligations.

### Ningi as a Data Processor

- Where the Personal Data breach affects data processed by Ningi as a Data Processor, the initial investigation shall establish whether a breach affecting the Data Controller’s data has occurred. If this is confirmed, Ningi shall notify the Data Controller as set out at Section 8.

### Ningi as a Data Controller

Where Ningi is processing the affected Personal Data as a Data Controller, the investigation shall also determine whether the breach is:

- unlikely to result in a risk to the rights and freedoms of Data Subjects
- likely to result in a risk to the rights and freedoms of Data Subjects; or
- likely to result in a high risk to the rights and freedoms of Data Subjects.

**Risks should be assessed objectively, from the Data Subject's perspective, using the risk matrix and guidance provided at Appendix 1.**

The decisions reached in the initial investigation must be documented in the Breach Assessment Form and signed-off by the Head of Performance and the DPO. The recommendation in the Breach Assessment Form should clearly set out one of the following conclusions:

- the Personal Data breach does not require notification to the ICO/relevant supervisory authority because there are no risks to rights and freedoms of Data Subjects; or
- the Personal Data breach requires notification to the ICO/relevant supervisory authority, because there are risks to rights and freedoms of Data Subjects; or
- the Personal Data breach requires notification both to ICO/relevant supervisory authority and to the affected Data Subjects because the risks to rights and freedoms of Data Subjects are high (except where measures have subsequently been taken to mitigate the high risk to Data Subjects, in which case notification to Data Subjects is not required); or
- where Ningi is acting as a Data Processor, whether the breach requires notification to the Data Controller.

#### **Notifying the ICO/relevant supervisory authority**

##### Ningi as a Controller

Unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of affected Data Subjects, Ningi shall report the Personal Data breach to the ICO/relevant supervisory authority without undue delay, and where feasible not later than 72 hours after having become aware of the Personal Data breach. Such notification shall only be made by the DPO following consultation with the Head of Performance.

Where a Personal Data breach notification to the ICO/relevant supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

At the time of notification, Ningi shall provide the following information to the ICO/relevant supervisory authority:

- a description of the nature of the breach;
- the categories of Personal Data affected;
- approximate number of Data Subjects affected;
- approximate number of Personal Data records affected;
- name and contact details of the Ningi DPO or alternative point of contact where a DPO has not been designated;
- details of the likely consequences of the breach;
- any measures that have been or will be taken to address the breach, including mitigation; and
- additional information relating to the data breach (additional information may be provided in phases after the 72 hour time limit provided reasons for the delay are provided).



## Notifying Affected Data Subjects

### Ningi as a Controller

#### Subsection A: Obligation to notify

Where the Personal Data breach is likely to result in a high risk to the rights and freedoms of affected Data Subjects, Ningi shall report the Personal Data breach to the affected Data Subjects without undue delay, except where Subsection B of this part applies. Such notification shall only be made by the DPO following consultation with the Head of Performance.

The notification to the data subject shall describe in clear and plain language the nature of the breach and must include:

- the name and contact details of the Ningi DPO where one has been designated, or other point of contact from whom more information may be obtained;
- a description of the likely consequences of the Personal Data breach; and
  - a description of the measures taken or proposed to be taken to address the Personal Data breach including, where appropriate, measures to mitigate its possible adverse effects.

The notification shall also offer advice to the Data Subjects regarding actions they may be able to take to reduce the risks associated with the Personal Data breach, where appropriate (e.g. advising that passwords should be reset where access credentials have been compromised).

The notification should be communicated to affected Data Subjects directly using a dedicated message, preferably email. Public communication may be used where communicating directly with every affected data subject would involve a disproportionate effort. Suitable public communications include prominent website banners or notifications and advertisements in print media.

**The notification communication must be signed-off by the Head of Performance and the DPO before it is shared with Data Subjects.**

#### Subsection B: When notification is not required

The obligation to notify Data Subjects affected by a Personal Data breach set out in Subsection A of this part shall not apply where:

- Ningi has implemented measures which render the affected Personal Data unintelligible to any person who is not authorised to access it (such as state-of-the-art encryption); or
- Ningi has taken steps following the breach which ensure that the high risk to the rights and freedoms of Data Subjects referred to in Subsection A of this part is no longer likely to materialise (such as immediately identifying and taking action against an individual who has access Personal Data before they were able to do anything with it).

## **Notifying the Controller**

### [ Ningi as a Data Processor]

Where the initial investigation establishes that a data breach has occurred which affects Personal Data processed by Ningi as a Data Processor, we shall notify the affected Data Controller of the breach without undue delay or within the timescale agreed with the Data Controller.

The notification to the Data Controller shall include but is not limited to:

- information about the nature of the incident including the date on which it occurred
- steps taken or proposed to mitigate the risks associated with the data breach
- categories of affected Personal Data
- volumes of affected Personal Data
- the potential consequences of the data breach
- contact details for Ningi 's Data Lead/DPO
- any other information the Data Controller requires, as set out in the data processing agreement.

## **Recording the Data Breach**

All Personal Data breaches shall be recorded in the Ningi Personal Data Breach Register, regardless of whether or not the breach needs to be notified to the ICO/relevant supervisory authority or to Data Subjects.

## **Implementation & Policy Management**

This procedure shall be deemed effective as of 10/03/2023. No part of this procedure shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This procedure will be reviewed annually and following any Personal Data breach by the Head of Performance and the DPO.

## Appendix 1 - Risk Matrix

<b>Severity of impact</b>	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		<b>Likelihood of harm</b>		

## Risk Assessment

Risk exists where the Personal Data breach may lead to physical, material, or non-material damage to the individuals whose data has been affected. Guidance can be sought from the DPO when assessing the risks associated with a Personal Data breach.

To assess whether a Personal Data breach is a high risk, consideration must be given to the likelihood and severity of the possible harm caused by the breach. Where a high risk to Data Subjects is identified, Ningi will notify the ICO/relevant supervisory authority] and Data Subjects in accordance with Sections 6 and 7 of this procedure. Where a medium risk is identified, the Head of Performance will consult with the DPO to determine next steps.

**Factors to be considered when assessing the risk to Data Subjects shall include:**

- the type of breach;
- the nature, sensitivity, and volume of Personal Data;
- ease of identification of individuals;
- severity of consequences for individuals;
- any special characteristics of the individual;
- the number of affected individuals.

A data breach involving 'Sensitive Personal Data' shall always be considered likely to result in a risk to Data Subjects and potentially a high risk, depending on the factors listed above.

**ROPA**

## Service Level Agreement

### Introduction

This Service Level Agreement (SLA) for Ningi Limited.

### Service Availability

Service hours – Ningi standard service hours are Monday to Friday, excluding bank holidays, between the hours of 9am to 5pm, however key communication lines are monitored outside of these hours.

Ningi Limited will use commercially reasonable endeavors to make the Service available 24 (twenty-four) hours a day, 7 (seven) days a week, excluding planned maintenance.

#### **Planned Maintenance**

Planned maintenance will be carried out during the maintenance window, which is scheduled between 10:00 pm to 2:00 am UK time. The Client acknowledges that during this period, the Service may be temporarily unavailable.

**Advance Notice:** In the case of unscheduled maintenance, Ningi Limited will use reasonable endeavors to provide the Client with reasonable advance notice, whenever possible.

#### **Response time**

Ningi Limited commits to responding to any queries, issues, or incidents raised by the Client in a timely manner during the service hours.

#### **Performance metrics**

**Uptime guarantee** - Ningi Limited aims to maintain a high level of uptime for the Service. In the event of any unplanned downtime, Ningi Limited will make commercially reasonable efforts to restore the Service promptly.

#### **Exclusions**

The parties recognise that certain events may be beyond the control of Ningi Limited, including but not limited to acts of nature, acts of terrorism, or other unforeseen circumstances. In such cases, Ningi Limited will not be held responsible for any service interruptions.

#### **Reporting**

The Client agrees to promptly report any incidents or issues related to the Service to Ningi Limited through the designated communication channels.

#### **Monitoring**

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

#### **Audit and Review**

##### **Internal Review**

Compliance with this policy will be monitored through Information Security Internal Audits, and by other management checks as required.

##### **External Review**

Inspections by external auditors may be carried out from time to time.

As part of these activities, external inspectors may ask to view internal records. Supervised access to such records must be provided where requested.

Copies of records must not be removed from site by an inspector unless this has been specifically approved by the ISMS Manager.

#### **Policy Review**

This policy will be reviewed by the ISMS Manager or his nominated delegate at regular intervals, not exceeding 1 year, or when business changes warrant it as part of the continual service improvement process.

## Data Leak Prevention Policy

### Introduction

This document sets out Ningi's commitment, to prevent the unauthorised extraction of sensitive information from networks, systems and other relevant devices by systems, individuals or other entities.

Consequently, Ningi will monitor networks, systems and other relevant devices within the constraints of applicable legislation and regulation to identify potential or actual data leakage.

### Applicability

This policy applies to all staff, including employees, contractors and interns working for or under the control Ningi.

### Scope

The scope of the policy includes the following type of information:

- ✓ Employee records;
- ✓ Financial corporate records;
- ✓ Intellectual property;
- ✓ Customer and supplier personal data.

### Policy

The unauthorised extraction of sensitive information includes the copying, transfer and export of information outside the boundaries of the organisation. This may include cloud services, email and removable media.

Where practicable, Ningi will implement controls necessary to restrict access to, and copy and export of sensitive information.

Where appropriate, Ningi will implement software tools to monitor systems, networks and other relevant devices to detect data leakage.

It is the responsible of all employees to report any potential or actual data leakage via the Information Security Incident Management Process.

## Legislative Compliance (security) Policy

### Purpose

Ningi has implemented an Information Security Management System (ISMS) in line with the ISO 27001 international standard for information security management.

In creating and maintaining an ISMS it is vital that a full understanding is gained of the various legal, regulatory and contractual requirements that apply to Ningi and its business. This will ensure that the organisation continues to meet its obligations and that its board of directors and other stakeholders are not exposed to the risk of criminal prosecution

or corporate liability.

The purpose of this policy is to document how such requirements are identified and incorporated into the ISMS and how updates to the requirements are handled.

### Applicability

This policy applies to all staff, including employees, contractors and interns working for or under the control of Ningi.

### Policy

#### Legal, Regulatory and Standard Compliance

Legal compliance relating to security is managed and audited at a number of levels:

- ✓ Senior Management review legal compliance at the ISMS Management Review meetings at least on a six-monthly basis.
- ✓ The ISMS Manager is responsible for day-to-day compliance matters, staff training and risk assessments.
- ✓ External and internal audit processes include a review of legal compliance, including the maintenance and accuracy of this policy.

#### Legislation and Regulations

Applicable Legislation	Further Information	Summary / Requirements	How Ningi meets its obligations
UK GDPR & Data Protection Act 2018	<a href="#">Link</a>	<p>The UK GDPR controls how personal information is used by organisations, businesses or the government.</p> <p>The Data Protection Act 2018 supplements, modifies and, in some cases, extends the UK GDPR.</p>	<ul style="list-style-type: none"> <li>• Ningi is registered with the ICO.</li> <li>• Data Protection Policy in place, supported by Data Protection Guidelines.</li> <li>• Confidentiality clause in staff Terms &amp; Conditions.</li> <li>• Training provided to staff on data protection.</li> <li>• Staff bound by Acceptable Use Policy</li> <li>• Data Protection built into contracts.</li> </ul>
The Privacy and Electronic Communications Regulations 2003 / 2011	<a href="#">Link</a> <a href="#">Link</a>	Support the Data Protection Act by regulating the use of electronic communications for the purpose of unsolicited marketing to individuals and organisations. Also provide rules on using calling-line identification, cookies, and directories.	All electronic direct marketing is reviewed and monitored by the Managing Director, who is a specialist in data protection and related ePrivacy compliance.
Computer Misuse Act 1990	<a href="#">Link</a>	Protects and secures computer material against unauthorised access and any harmful type of	<ul style="list-style-type: none"> <li>• Acceptable Use Policy.</li> </ul>



		modification. 3 offences: unauthorised access; unauthorised access with intent to commit or facilitate commission of further offences; unauthorised modification. Main purpose is to prevent copyright infringements, hacking, using computer data for fraud or blackmail, the creation of viruses and the illegal deleting or altering of computer data	<ul style="list-style-type: none"> <li>• System monitoring &amp; controls, Anti-virus, etc.</li> <li>• Access Controls.</li> <li>• Staff training.</li> <li>• Internal development guidelines.</li> <li>• Anti-Bribery policy and processes.</li> <li>• Governance and escalation processes.</li> <li>• Back-up and restoration processes.</li> <li>• Protective Monitoring Policy.</li> <li>• Clients required to sign 'Permission to Test' form when we carry out computer security tests</li> </ul>
The Human Rights Act 1998	<a href="#">Link</a>	Codifies human rights including the right to privacy and to a personal life.	<ul style="list-style-type: none"> <li>• Data Protection Policy</li> <li>• Privacy Notices</li> <li>• Designation of a Data Protection Manager</li> </ul>
Copyright, Designs and Patents Act 1988	<a href="#">Link</a>	Prohibits the copying of software and manuals and any action that contravenes the conditions of the software license	<ul style="list-style-type: none"> <li>• No unauthorised software can be copied onto company owned equipment.</li> </ul>
Copyright (Computer Programs) Regulations 1992	<a href="#">Link</a>	The Copyright (Computer Programs) Regulations 1992 extended the rules covering literary works ("Copyright, Designs and Patents Act 1988") to include computer programs.	<ul style="list-style-type: none"> <li>• Copying software to other computers is illegal. Ningi and its users may be prosecuted under the Act, with penalties and fines and possible imprisonment and compensation payments to the software companies concerned.</li> </ul>
Civil Evidence Act 1995	<a href="#">Link</a>	Compliance regarding evidence in civil and criminal cases.	<ul style="list-style-type: none"> <li>• Doesn't apply directly, but Ningi has policies in place to secure and protect data – Logging and Monitoring Policy.</li> </ul>
Police and Criminal Evidence Act 1984	<a href="#">Link</a>		
Regulation of Investigatory Powers Act (RIPA) 2000	<a href="#">Link</a>	Came into force in October 2000. Section 49 includes a provision for public authorities	<ul style="list-style-type: none"> <li>• Cryptography policy states that anyone who could be</li> </ul>

		to demand, where it is judged there are reasonable grounds, decryption keys or decryption of information stored on computer systems in the UK.	assumed to have encrypted and stored data is very strongly advised to ensure that they retain the means to decrypt it.
Companies Act 2006	<a href="#">Link</a>	Sets out company law, codifies directors' duties and describes sets out shareholder rights.	<ul style="list-style-type: none"> <li>• Directors adhere to the company Articles of Association and Companies Act legal obligations, with advice from professional advisers if required.</li> </ul>
Waste Electrical and Electronic Equipment (WEEE) Regulations 2013	<a href="#">Link</a>	Provides guidance on the disposal of waste electrical / electronic equipment. Relevance to Ningi is primarily with regards to the disposal of laptops.	<ul style="list-style-type: none"> <li>• Ningi follows the WEEE regulations when disposing of obsolete laptops and other computer peripherals that fall within the scope of the regulations.</li> </ul>
Health and Safety at Work etc. Act 1974	<a href="#">Link</a>	Guidance on how to comply to health and safety laws in the work environment. It is the primary piece of legislation covering occupational health and safety in Great Britain.	<ul style="list-style-type: none"> <li>• Ningi is committed to following relevant Health and Safety regulation for the protection of its employees</li> </ul>
Employers' Liability (Compulsory Insurance) Act 1969	<a href="#">Link</a>	The act requires employers to insure against their liability for personal injury to their employees	<ul style="list-style-type: none"> <li>• Ningi is insured and the insurance certificate is displayed in the office. Copy can be requested via email to any of the Directors.</li> </ul>
RIDDOR - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013	<a href="#">Link</a>	RIDDOR puts duties on employers, the self-employed and people in control of work premises (the Responsible Person) to report certain serious workplace accidents, occupational diseases and specified dangerous occurrences (near misses).	<ul style="list-style-type: none"> <li>• Ningi is committed to ensuring that it protects its employees and visitors by complying with the requirements of the act.</li> </ul>
Immigration Act 2016	<a href="#">Link</a>	This act puts duties on employers to ensure that they only recruit individuals that are legally entitled to work in the UK.	<ul style="list-style-type: none"> <li>• Ningi ensures that it only employs individuals that are legally entitled to work in the UK. The Right to Work in the UK of all new starters is systematically checked as part of the recruitment process.</li> </ul>
The	<a href="#">Link</a>	These Regulations authorise	<ul style="list-style-type: none"> <li>• Where relevant,</li> </ul>

Telecommunications (lawful Business Practice and Interception of Communications) Regulations 2000		certain interceptions of telecommunication communications which would otherwise be prohibited by section 1 of the Regulation of Investigatory Powers Act 2000.	Ningi is committed to following requirements set out by this act.
The Electronics Signatures Regulations 2002	<a href="#">Link</a>	The provisions of this Directive which are implemented relate to the supervision of certification-service-providers, their liability in certain circumstances and data protection requirements concerning them; provisions in the Directive relating to the admissibility of electronic signatures as evidence in legal proceedings were implemented by section 7 of the Electronic Communications Act 2000	<ul style="list-style-type: none"> <li>• Ningi is committed to ensuring that employees are following relevant guidance set out by this act.</li> </ul>
The Information and Consultation of Employees Regulations 2004 (ICE)	<a href="#">Link</a>	These Regulations, made under powers in section 42 of the Employment Relations Act 2004 implement in Great Britain Directive 2002/14/EC establishing a general framework for informing and consulting employees in the European Community	Ningi is committed to ensuring that relevant requirements of the regulations are followed by company directors.
Pension Schemes Act 2021	<a href="#">Link</a>	An Act to make provision about pension schemes, including provision designed to encourage arrangements that offer people different levels of certainty in retirement or that involve different ways of sharing or pooling risk and provision designed to give people greater flexibility in accessing benefits and to help them make informed decisions about what to do with benefits.	<ul style="list-style-type: none"> <li>• Directors are committed to ensuring that all staff are covered under the requirements of the act.</li> </ul>
Bribery Act 2010	<a href="#">Link</a>	An Act to make provision about offences relating to bribery	<ul style="list-style-type: none"> <li>• Ningi is committed to ensuring that all staff are aware of the precautionary actions and the potential ways in which bribery can occur. Ningi ensures that staff receive appropriate training during their induction and at least annually thereafter</li> </ul>
Communications Act	<a href="#">Link</a>	An Act to confer functions on	<ul style="list-style-type: none"> <li>• Ningi is committed</li> </ul>

2003		the Office of Communications; to make provision about the regulation of the provision of electronic communications networks and services and of the use of the electro-magnetic spectrum; to make provision about the regulation of broadcasting and of the provision of television and radio services; to make provision about mergers involving newspaper and other media enterprises and, in that connection, to amend the Enterprise Act 2002	to ensuring that the relevant requirements of this act are followed by employees.
Employment Act 2008	<a href="#">Link</a>	An Act to make provision about the procedure for the resolution of employment disputes; to provide for compensation for financial loss in cases of unlawful underpayment or non-payment; to make provision about the enforcement of minimum wages legislation and the application of the national minimum wage to Cadet Force Adult Volunteers and voluntary workers; to make provision about the enforcement of offences under the Employment Agencies Act 1973; to make provision about the right of trade unions to expel or exclude members on the grounds of membership of a political party	<ul style="list-style-type: none"> <li>• Ningi is committed to ensuring that the requirements set out by this act are met by the organisation.</li> </ul>
Equality Act 2010	<a href="#">Link</a>	An Act to make provision to require Ministers of the Crown and others when making strategic decisions about the exercise of their functions to have regard to the desirability of reducing socio-economic inequalities; to reform and harmonise equality law and restate the greater part of the enactments relating to discrimination and harassment related to certain personal characteristics; to enable certain employers to be required to publish information about the differences in pay between male and female employees; to prohibit victimisation in certain circumstances; to require the	<ul style="list-style-type: none"> <li>• Ningi is committed to ensuring that employees comply with the requirements set out by this act. During the screening part of the Recruitment process steps are taken to ensure everyone is treated equally.</li> </ul>

		exercise of certain functions to be with regard to the need to eliminate discrimination and other prohibited conduct; to enable duties to be imposed in relation to the exercise of public procurement functions; to increase equality of opportunity; to amend the law relating to rights and responsibilities in family relationships.	
Malicious Communications Act 1988	<a href="#">Link</a>	An Act to make provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety.	<ul style="list-style-type: none"> <li>• Ningi is committed to complying with the relevant requirements of the act.</li> </ul>
Modern Slavery Act 2015	<a href="#">Link</a>	An Act to make provision about slavery, servitude and forced or compulsory labour and about human trafficking, including provision for the protection of victims; to make provision for an Independent Anti-slavery Commissioner.	<ul style="list-style-type: none"> <li>• Ningi is committed to ensuring that no employee will fall below the requirements of this act.</li> </ul>
The Electronic Commerce (EC Directive) Regulations 2002	<a href="#">Link</a>	These Regulations implement Articles 3, 5, 6, 7(1), 10 to 14, 18(2) and 20 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.	<ul style="list-style-type: none"> <li>• Where relevant, Ningi is committed to ensuring that the requirements set out in this act are followed by all employees.</li> </ul>
The Provision and Use of Work Equipment Regulations of 1998	<a href="#">Link</a>	These Regulations impose health and safety requirements with respect to the provision and use of work equipment, which is defined in <i>regulation 2(1)</i> .	<ul style="list-style-type: none"> <li>• Ningi is committed to ensuring the health and safety of their employees in accordance with these regulations through the use of our Display Screen Equipment (DSE) Workstation Checklist.</li> </ul>
The Management of Health and Safety at Work Regulations of 1999	<a href="#">Link</a>	These Regulations re-enact the Management of Health and Safety at Work Regulations 1992, with modifications regarding new regulations and the revoking of others.	<ul style="list-style-type: none"> <li>• Ningi is committed to ensuring that the Health and Safety of staff is well maintained and follow all relevant requirements of the act.</li> </ul>

## Standards and Frameworks

Applicable Standards and Frameworks	Further Information	Summary / Requirements	How NINGI Meets its obligations
ISO 27001	<a href="#">Link</a>	International standard setting out requirements for an auditable information security management system designed to achieve best practice regarding the maintaining data integrity, safeguarding confidentiality, and controlling availability.	<ul style="list-style-type: none"> <li>• NINGI ISO 27001 certification</li> <li>• Management Review</li> </ul>