Information Security Policy

Assembly Managed Services

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

POLICY TITLE	Information Security Policy		
ISSUE DATE	30/06/2025	**REVIEW DATE**	27/06/2026
VERSION	1.2	**ISSUED BY**	James Reilly

ASSOCIATED DOCUMENTS	Data Protection Impact Analysis (DPIA); Change Management Process; New User Process; Leaving User Process; Business Continuity Plan;

APPROVED BY	Peter Smith (Managing Director)	**DATE**	30/06/2025

REVIEW AND CONSULTATION PROCESS	This policy will be reviewed by the board of directors at least annually and by the Director of Technology as required. Changes and amendments will be review by the board and authorised for release at quarterly review meetings.

RESPONSIBILITY FOR IMPLEMENTATION AND TRAIN-	The Director of Technology, James Reilly is responsible for the implementation of this policy and the training of staff in relation to the topics covered within the policy.

REVISION	DATE	AUTHOR	DESCRIPTION
0.1	28/06/2022	James Reilly	Initial Draft for review
0.2	29/06/2022	James Reilly	Update post initial review
1.0	30/06/2022	James Reilly	Initial Release
1.1	30/06/2024	James Reilly	Updated dates post annual review
1.2	30/06/2025	James Reilly	Reviewed and amended CRM name

DISTRIBUTION	Document will be made available to all staff in Microsoft Teams (from SharePoint Folder where it is published) as Read-Only Version

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

Contents

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

INTRODUCTION

This Information Security Policy (SECPOL) is a key component of Assembly Global Networks business management framework and is designed to set out the requirements and responsibilities for maintaining the security of information within the business. The policy is supported by other policies and by guidance documents to assist in putting the policy into practice day-to-day.
Whilst Assembly Global Networks do not generally work with any data partners, it is expected that any partners who are authorised to work with Assembly Global Networks will also comply (and are expected to comply) with the requirements of this policy in any dealing with Assembly Global Networks.
This policy is in relation to the systems utilised by Assembly Global Networks for the delivery of services to our clients and where partners are delivering services directly to Assembly Global Networks Clients and not interacting or utilising Assembly Global Networks systems, they will not be expected to adhere to this policy.

AIM AND SCOPE OF THIS POLICY

The aims of this policy are to set out the rules governing the secure management of Assembly Global Networks information assets by:

- Preserving the confidentiality, integrity, and availability of our business information
- Ensuring that all members of staff (and any authorised contractors) are aware of and fully comply with the relevant legislation as described in this and other policies
- Ensuring an approach to security in which all members of staff fully understand their own responsibilities
- Creating and maintaining within the organisation a level of awareness of the need for information
- Detailing how to protect the information assets under our control
- Creating an understanding of how to work with the technology and systems provided to deliver our services in a secure and risk adverse manner.

This policy applied to all information assets, data information systems, networks, applications, locations (both office, home office and mobile) and staff of Assembly Global Networks and/or contractors or services supplied under contract to Assembly Global Networks.

The policy is designed to be read as both our Information Security Policy and our generic acceptable use policy covering the use of the systems, services, and devices within this document; further acceptable use and process documents may be utilised for specific systems, such as:

- NinjaOne (incorporating RMM and Service Ticketing)
- Corporate Websites
- Microsoft 365 (including Email, Teams, OneDrive, SharePoint)

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

RESPONSIBILITIES

Ultimate responsibility for information security rests with the Managing Director (Peter Smith) of Assembly Global Networks, but on a day-to-day basis the Director of Technology, (James Reilly) shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this policy, the Business Information Risk Register (Data Protection Impact Analysis – DPIA) and for recommending appropriate risk management measures is held by the Director of Technology (James Reilly). Both this policy and the DPIA shall be reviewed at least annually by the Director of Technology.

Line Managers are responsible for ensuring that their permanent staff, temporary staff, and contractors are aware of:

- The information security policies applicable to their work area's
- Their personal responsibilities for information security
- How to access advice on information security matters

KEY NOTES

- All staff shall comply with the information security policy and must understand their responsibilities to protect the Assembly Global Networks' data. Failure to do so may result in disciplinary action.
- Line managers shall be individually responsible for the security of information within their business area.
- Each member of staff shall be responsible for the operational security of the information systems they use.
- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity, and availability of the information they use is maintained to the highest standard.
- Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

LEGISLATION

Assembly Global Networks is required abide by certain UK, European Union, and international legislation. It also may be required to comply to certain industry rules and regulations.
The requirement to comply with legislation shall be devolved to employees and agents of Assembly Global Networks, who may be held personally accountable for any breaches of information security for which they are responsible.
Assembly Global Networks is required to comply with:

- The Data Protection Act (2018)
- General Data Protection Regulations (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- The Health and Safety at Work Regulations 1999
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Bribery Act 2010
- Public Interest Disclosure Act 1998

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

PERSONAL SECURITY

CONTRACTS OF EMPLOYMENT

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause
- References for new staff shall be verified and a passport, driving license or other documentation shall be provided to confirm identity
- Information security expectations of staff shall be included within appropriate job descriptions
- Whenever a staff member leaves the company, their accounts will be disabled the same day, they leave

INFORMATION SECURITY AWARENESS TRAINING

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice or risk taking are reduced
- Information security awareness training shall be included in the staff induction process and shall be carried out at least annually for all staff
- An on-going awareness programme shall be established and maintained to ensure that staff awareness of information security is maintained and updated, as necessary.

INTELLECTUAL PROPERTY RIGHTS

- Assembly Global Networks shall ensure that all software is properly licensed and approved by the Director of Technology (James Reilly).
- Individual and Assembly Global Networks intellectual property rights shall be always protected.
- Users breaching this requirement may be subject to disciplinary actions.

ACCESS MANAGEMENT

PHYSICAL ACCESS

- Only authorised personnel who have a valid and approved business need shall be given access to area's containing information assets (information systems, applications, and stored data)
- Where indicated by a risk assessment, access to the network will be restricted to authorised devices

LOGICAL ACCESS

- Access will only be via a unique username and password combination (see Identity and passwords below)
- Usernames and Passwords will not be shared and will be unique per-employee

- If an employee must share a password with the support team for support purposes, they will immediately change that password when support concludes, or may change the password to something else to provide to support and then revert to their original password after support concludes.
- No shared accounts will be used to access any information assets (devices, information systems, databases, email, and other similar systems)

IDENTITY AND PASSWORDS

- Passwords must offer an adequate level of security to protect systems and data
- Passwords must be at least 8 Characters in length, contain alpha-numeric characters and special symbols
- All systems will be configured to utilise Multi-Factor Authentication where this is supported by the system, application, or vendor – ***employee's will ensure that multi-factor authentication is utilised where it is available*** and must not disable the service once its enabled.
- Passwords will be generated "securely" for new employee's and should be changed on first use.
- Self-Service Password Reset solutions will be used where the system being used supports that capability – employees are required to enrol on any "self-service" solution that is made available to them.

PASSWORD GUIDENCE

A good password is something that is not only difficult for a person to guess but is also something that would take a computer-based attack some considerable time and effort to crack. There are some basic "good practices" for choosing a password, such as:

- The longer the password the better
- Ensure you utilise
    - Upper Case / Lower Case
    - Numbers
    - Symbols
- Consider using a phrase which you can remember and chaining words together and perhaps replacing characters, such as an E becoming a 3 and adding some special characters such as an @ for an A and also ending the password with a few special characters! $%. MyH0u5315Numb3r12 or TheBrownFoxWasPink!

DEVICE PINS / WINDOWS HELLO / BIOMETRICS / MOBILE PINS

- Mobile devices will utilise at least an 8-digit pin
- Biometrics, including Windows Hello can be used by the underlying PIN must comply with at least 8 digits

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

USER ACCESS

- Access to information systems will be provided on a “least privileged” basis to all systems.
- Access to information systems will be restricted to those authorised users who have a legitimate business need.
- Requests for additional access will be authorised by the Information Asset Owner (IAO) of each individual system as they are responsible for the security of the systems, they are the asset owner for. IAO’s for systems are recorded in the companies DPIA (Data Protection Impact Analysis) Document.
- A business case / role-based access need is required before any access to an information asset is provisioned.
- The IAO will be responsible for reviewing the users who have live access to the system and their appropriate access rights to the data located within that system on at least an annual basis.
- Request for permission increases or changes is to be made to the IAO of the system and they will ultimately decide about provision of access, referring to the board if required and ensuring there is a valid business case for the change to be made.
- The IAO is responsible for ensuring that users who no longer require access are removed from the system.
- Any changes to IAO’s or indeed the access needs of any person are to be actioned only after a duly authorised ticket is logged and completed within the Internal Service Request System.

ADMINISTRATIVE ACCESS

- Administrative access will only be provided to any information asset by the Information Asset Owner (IAO) following board approval.
- Like standard accounts, Administrative accounts MUST utilise Multi-Factor Authentication, if available.
- IAO’s will review, at least annually, who has administrative access to their systems.
- All requests for administrative access are to be logged within Internal Service Request System and must be authorised by a board member / director before being actioned.
- Administrative accounts will never be used to access the Internet or Email and any required downloads should be completed using a standard user account; after download, elevation should be used to allow administrative access in preference to interactive login to any system.
- Any user with an administrative account will ensure their account is only ever used for elevation and will only login interactively if essential. Day to day access will always be via the standard user account.

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

ACCESS REVIEWS

- Information asset owners will complete a review of the users who have access to their Information Assets at least annually, this will include a review of who has administrative access to the information assets.

SYSTEM PERIMETER ACCESS (FIREWALLS)

- All internet connections will be protected by physical firewall devices, either individual firewalls behind the ISP Router or integrated firewall systems within the ISP router.
- All devices, phones, tablets, laptops, PC's and alike will, where options are available, have software firewall's enabled and users will ensure that these remain active and always switched on.
- Firewalls will be configured to block all inbound connections by default unless there is a documented business case for any open inbound connection – where temporary, open connections will be removed as soon as possible after opening and managed through the Internal Service Request within the ticketing system.

STAFF WORKING FROM HOME (FIXED OR TEMPORARILY)

- Staff working from home do so on the understanding that they will ensure:
    - The default administrative password on their ISP provided router has been changed
    - The password is at least 8 characters in length and is complex and hard to guess
    - The router does not have remote administration enabled
    - The firewall on the device is locked to ensure that it does not allow any inbound access to the internal network or systems.
    - The WIFI password has been changed from the default provided by the ISP router
- By signing this policy and/or further policies regarding home working, employees and contractors agree they will have already aligned their systems to the above requirements.
- Assembly Global Networks reserve the right to check and confirm the above given reasonable (48 hours, working day access) notice to the employee.

Note: *If an employee requires ports to be opened for any reason, they should check this with the Director of Technology to ensure this can be delivered safely and without risk to both the home environment and our corporate systems. In general, we expect to be able to record any request as "authorised" within our risk register and thus record a "business case" for the port to be open and only on rare occasions will we require the home user to cease use of the open port whilst we review risk mitigation actions / options.*

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

MOBILE WORKING

Staff wishing to work mobile should consider the safety implications of their location and the method of connection being used on the device to access the Internet and cloud-based services. Special consideration should be taken when accessing Assembly Global Networks Systems (which may be in the background and out of user direct control) to ensure the safety of our systems and environment.

If working remotely we require you to:

- Use your smart phone to provide tethered internet access to your device
- DO NOT use public or shared WIFI on your device
    - If for any reason you believe there is a critical need to use public WIFI or Shared WIFI a VPN should be used to further encrypt the traffic and ensure that no-one is able to intercept any traffic from your device to the Assembly Global Networks systems. The Director of Technology can provide access to a VPN if this is required but is not provided by default.
- Ensure that every system you have, and use complies with all other aspects of this policy, especially Password and Multi-Factor Authentication requirements.
- Be always aware as to the location of your device, ensure it is logically locked if you leave it for any reason (even storing in your bag) and never leave it unattended (without another Assembly Global Networks employee having oversight), whether in a coffee shop, train or elsewhere.

DEFAULT PASSWORDS / SETTINGS (ALL DEVICES)

It is essential that all default passwords are changed from those which the device ships with from the factory or from the default installation settings of any software application. Assembly Global Networks will require any staff involved in the configuration of equipment, or users utilising any Bring Your Own Device (BYOD) devices (including Home Working) to ensure that all default passwords have been changed, these include:

- Factory Shipped Router Password
- Factory Shipped WIFI PSK/WPA Keys
- Inbuilt Guest Account (disabled, but ensure password changed)
- Inbuild Administrative/Root Account (rename if possible, change password and ideally disabled)
- SNMP Community Strings (change from default)
- Other device management passwords (e.g., UPS / Switch)

NOTE: *Passwords generated by machines (i.e., those printed on routers) that appear to be secure can of course be re-created by a machine if the algorithm is known, therefore, the appearance of a strong password is not confirmation of a strong password. ALL default passwords, regardless of appearance, should be changed before the device is used.*

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

MONITORING SYSTEM ACCESS AND USE

- Where supported and available by the information system, a full audit trail will be recorded and reviewed on a regular basis. Monitoring will generally be completed through our Security Incident and Event Management (SIEM) platform which retains all log information for 90 days.
- Assembly Global Networks reserves the right to monitor systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000) or for personnel training reasons.
- Assembly Global Networks will install specific management tools onto your device (this may include requiring you to install these tools if a BYOD solution is agreed) and you should not alter the configuration of these tools in any way.
- There should be no expectation of privacy when utilising any Assembly Global Networks Information Asset or any device accessing Assembly Global Networks Systems.

ENCRYPTION / REMOTE DATA WIPE

All devices in use by users, whether mobile phones, tablets or any other device must be:

- Protected with a password in line with the policy within this document
- Encrypted from boot/start up, for entire device, not just data area's (this is default by policy on the first use of any Assembly Global Networks device following the first sign-in of any Assembly Global Networks user account)
- If a mobile, only access Assembly Global Networks systems using the Company Portal Application which will create an isolated work profile on the device which is controlled by Assembly Global Networks outside of any end-user applications or services. Using the Company Portal Application on a mobile ensures that:
    - Company data is isolated away from any of your personal data
    - Email access is within the work profile and does not bleed out to the personal profile
    - Work Calendar access can Synchronise on the local calendar as well as work profile
    - Work Contacts can Synchronise on the local contacts to allow calling
    - We can remotely wipe "our" Assembly Global Networks Work Profile on the device leaving anything of your private data on the device
    - We can manage the applications installed in the work profile to ensure you only use (for work) what we control
    - We will review your Operating System / Patching to ensure that your device is up to date and compliant with required standards
    - We will enforce an 8-digit pin on the work profile on your device.
- Users who wish to utilise BYOD for mobile phone access (to access email, calendars etc) must comply with this policy as well and will be expected to accept the required policies pushed out from Assembly Global Networks systems onto their device generating the Work Profile by installing the Company Portal Application. Installation of the Company Portal Application to access Company Data confirms your acceptance to the policy.

ASSET MANAGEMENT

ASSET OWNERSHIP

- Each individual asset (hardware, software, application, or data) shall have a named custodian who shall be responsible for the information security of that asset.

ASSET RECORDS AND MANAGEMENT

- An accurate record of business information assets, including source, ownership, modification, and disposal shall be maintained.
- All data shall be securely wiped from all hardware before disposal.
- Devices will have the Asset Inventory Application (Intune) installed to allow easy capture of device information.

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

ASSET HANDLING

ASSET CLASSIFICATION

- Assembly Global Networks shall identify particularly valuable or sensitive information assets using data classification (below).
- All staff are responsible for handling information assets in accordance with this security policy.
- All company information shall be categorised into one of the three categories as listed in the table below.

CATEGORY	DESCRIPTION	EXAMPLE
PUBLIC	Information which is not confidential or restricted and can be shared with anyone and any channel	▪ Details of products and services on our website ▪ Published company information ▪ Social media updates ▪ Press releases
CLIENT ONLY	Information generated from our assessments and working with clients which is strictly confidential between Assembly Global Networks and the Client. The exception to Assembly Global Networks and Client confidentiality is where we are working with a client with a partner/contractor/agency, where the confidentiality chain exists between {company name}, our/clients partner/contractor/agency and the end-client.	▪ Project details / Project Information ▪ Work requests ▪ Contracts for the delivery of services ▪ Commercial Agreements ▪ Non-Disclosure Agreements
INTERNAL	Information which, if lost or made available to unauthorised persons could impact the company's effectiveness, benefit competitors or cause embarrassment to the organisation and/or its partners/clients	▪ Company operating procedures ▪ Client Contact Details ▪ Company plans / financials ▪ Employee Salary Information ▪ Any data classed as "Sensitive personal data" under the Data Protection Act / General Data Protection Regulations.

- Assembly Global Networks are 100% electronic in terms of service delivery and management systems and therefore do not generally utilise "paper" systems, however, in the event paper documents are stored, they will be marked according to the classifications detailed above and stored with a level of security akin to the level of confidentiality highlighted above.

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

ASSET CLASSIFICATION DATA SEGREGATION

- Assembly Global Networks utilise our platforms to segregate data ensuring that it is easy to identify data that is “Public” and can be shared, “Internal” and cannot be passed to anyone outside of Assembly Global Networks and of course, “Client” which cannot be shared with anyone except the Client and those staff internally who need to have access to the information.
    - Assembly Global Networks work with “Partners” for the delivery of services to their clients, therefore “Client” can be either the end-user-client or the “Partner/Contractor” who we are working with to deliver services to the end-client.

CATEGORY	SYSTEM	NOTES
PUBLIC SYSTEMS	▪ Assembly Global Networks Website	Content that is made available for release to clients will be stored in the partner area of the website. Content for general release will be stored in open access area’s on the website
CLIENT ONLY SYSTEMS	▪ Electronic Signature ▪ Stripe ▪ LinkedIn ▪ Project Management ▪ Shared Data Storage	Information stored within these systems should remain confidential and access to information for a client should only be to their own information and only then if there is a requirement to provide that information.
INTERNAL SYSTEMS	▪ CRM ▪ Accounting ▪ Project Management ▪ Help Desk ▪ SharePoint ▪ Teams ▪ Email Systems ▪ OneDrive for Business ▪ HR System	Internal systems contain a mix of data and for ease, it should be assumed that all data stored within these systems is for Internal Consumption only and there is no authorisation to share this data. The exception to this rule will be marketing documents which are stored in SharePoint (presented in teams) and are shown as “shareable” in the area they are stored.

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

REMOVABLE MEDIA

In general, there is no requirement for the use of removable media for the storage or transport of any data, however, these may be used for the transportation or distribution of data classified as “Public”. Assembly Global Networks systems are however automatically configured to require encryption for any USB write, therefore if you have a USB that you wish to write data to, you will have to Bit-locker (system will prompt you) the device before you can write data to it.
Where indicated by risk assessment, systems may be prevented (logically or physically) from having access to removable media.
In the unlikely need that removable media is required for data transit, employee’s will seek the advice of the Director of Technology (James Reilly) to review the security requirements and risks around the required data set and its transportation. All media holding non-public data will be encrypted using BitLocker encryption.

PERSONAL DEVICES / BRING YOUR OWN DEVICE (BYOD)

Assembly Global Networks may support the use of Bring-Your-Own-Device where there is a valid business reason – BYOD will not be used as “the normal” and employee’s will be provided with company devices to carry out their day-to-day business operations.

Any person who wishes to utilise a BYOD device will be required to comply with the stringent policies required for any device being used to access Assembly Global Networks systems, these include but are not limited to:

- No shared accounts on the system
- Default user accounts have been changed / removed / disabled or protected in another way
- Device is running an approved operating system and applications
- Applications not authorised by {company name} are to be removed and not re-installed
- Device is not used for Torrenting or similar online streaming services
- User of the system is not a local administrator for day-to-day use
- Home working policy requirements detailed earlier are in place at the home location where the BYOD device generally resides.
- The BYOD user confirms that they will ensure all applications are patched and up to date at least weekly or will enable the installation of the {company name} patch management application to allow Assembly Global Networks to maintain patching on the device.
- Assembly Global Networks will provide a “local user copy” of our Zero Trust security software to be installed to deliver enhanced protection to the device – whilst you will be able to disable this for up to 10 minutes, you are required to ensure that the software remains active as soon as you complete any administrative functions on your BYOD device that required the protection to be paused.
- Assembly Global Networks will provide a copy of our SIEM software to be installed onto your BYOD device to ensure that the solution is monitored for threats and other issues and to ensure we are always aware of the compliance status of the device. This software is to remain on

the device whilst being used for any {company name} business and is not to be removed for any reason. Assembly Global Networks

- Working from home on any BYOD device on Assembly Global Networks systems confirm your acceptance to this policy.

Assembly Global Networks reserve the right to decline any request for use of a BYOD device and remove any previously given permission at any time, without notice or explanation.

Permission for BYOD will not be given for any user who is delivering services directly on client sites or linking into client systems or other delivery area's where a device may be used to compromise a client's system or clients network.

AUTORUN

Autorun is disabled by policy on all Assembly Global Networks devices, if you authorised to use a BYOD device, which is not configured to block auto-run you are required to disable this feature.

SOCIAL MEDIA

- Social Media may only be used for business purposes by using official business social media accounts with authorisation from either the Managing Director (Peter Smith) or Director of Technology (James Reilly). Users of business social media accounts shall be appropriately trained and aware of the risks of sharing sensitive information via social media.
- Business social media accounts shall be protected by strong passwords and where available multi-factor authentication.
- Users shall have the responsibility while using any social media whether for business or personal use, bearing in mind they directly or indirectly represent the company. If in doubt, consult the Managing Director (Peter Smith) or the Director of Technology (James Reilly).

PHYSICAL AND ENVIRONMENTAL MANAGEMENT

- To protect our devices and minimise the threats from loss and environmental damage, appropriate security measures should be put in place.
- Users working from their home offices should ensure that devices are always protected and when left securely at home, are logically locked (not logged in) and placed out of direct access for anyone who may enter the premises.
- When travelling with devices (see mobile working) devices must be always kept secure.
- Subject to a risk assessment identifying a need, devices may require additional protection such as:
    - Uninterruptible Power Protection
    - Air Conditioning and Environmental Alerting

  Systems requiring specific needs, such as environmental conditions, will be provided with solutions to ensure they remain working in an optimal environment. Any such requirements will be reviewed by the Director of Technology (James Reilly)

COMPUTER AND NETWORK MANAGEMENT

OPERATIONS MANAGEMENT

- Management of computers, networks and systems will be managed through standard documented procedures that have been authorised by the Managing Director (Peter Smith) and/or the Director of Technology (James Reilly)

SYSTEMS CHANGE CONTROL

- Any information system requiring a change will be subject to an authorised change control which will be processed through the Assembly Global Networks Change Management Process (see additional process document) which requires requests to be logged within our ticketing system, examples of which are:
    - Adding a user (New User Process)
    - Removing a user (Leaving User Process)
    - Job Role Change (Change Control also referencing Access Rights)
    - Access Rights Change (Change Control)
    - Administration account provision

ACCREDITATION

- Assembly Global Networks will ensure that all new and modified information systems, applications, and networks include security provisions and comply with any relevant legislation or legal obligations of Assembly Global Networks as relevant at the time.
- Systems will be correctly sized, designed with security first in mind and changes approved by the Director of Technology (James Reilly) before being brought into production.

SOFTWARE MANAGEMENT

- All application software, operating systems and firmware will be updated on a regular basis to reduce the risks presented by security vulnerabilities.
- All application and operating system and firmware updates listed as High-Risk or Critical will be installed within 7 days of patch/update release.
- Generally, all software application and operating system updates will be deployed to devices within 7 days of release.
- Patching will be managed by the Assembly Global Networks Patch Management System (what system is in use and how is it configured).
- Only where there is a business case for use will software be installed on any end-user device.
- Any un-used or not-required software will be removed from the device as part of the build process.

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

- Users shall not install any software or other active code onto their devices without the express permission of the Managing Director (Peter Smith) or Director of Technology (James Reilly) utilising the Change Control Process. (Installation of any unauthorised applications will be blocked by the Assembly Global Networks, Zero Trust software protection solution and the "Break Glass" password will be held only by the Director of Technology (James Reilly)
- Software installation will be completed via the software deployment tools and will not be deployed directly on the device; it is unlikely that there is any software which cannot be "package deployed" and this will be completed even if only a single user requires the software.

LOCAL DATA STORAGE / BACKUP

- OneDrive for Business will be used on all devices to replicate known folder data into the Microsoft 365 Data Centre (our backup) which also has support for anti-malware / anti-crypto attacks. Users will ensure that this solution is working and in place and will not change the settings once working. OneDrive for Business replication of known folders is configured by policy to activate after first login for all users on any device.
- Assembly Global Networks will utilise a 3rd Party Backup solution to protect the information assets stored within Microsoft 365 to ensure we have longer backup protection windows than that afforded by Microsoft.
- Our Microsoft 365 information assets will be backed up daily (retention 7-days, 4-weekly, 2 monthly) with server/system images taken and retained for 2 days (2 images) for fast restoration of services in the event of failure.

EXTERNAL CLOUD SERVICES

- Where data storage, applications or other services are provided by another business (e.g., a 'cloud provider') there must be independently audited, confirming that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.
- Systems (such as CRM and Customer Cloud Shares) provided under a Software as a Service (SaaS) agreement will be reviewed in terms of data retention and backup/recovery to determine whether additional backup solutions are required

PROTECTION FROM MALICIOUS SOFTWARE

- Assembly Global Networks will utilise NinjaOne with the Bitdefender engine as our Zero Trust solution on all devices. This solution will offer greater protection to the devices and will be used (to comply with current Cyber Requirements) with Windows Defender or other relevant Anti-Virus Solutions to align completely to and more than the current UK Cyber Security Standards. NinjaOne with the Bitdefender engine will be centrally administered, and users will not have the ability to prevent its operation.
- The "Break Glass" password will be held only by the Director of Technology (James Reilly).

- NinjaOne (Zero Trust) will be installed by policy on any device for each user after first logon and cannot be removed without the Break Glass password.

DETECT AND PROTECT (SOC/SIEM)

- Assembly Global Networks will utilise a Security Operations Centre for the provision of SOC services which will receive 24/7/365 alerting from our Security Incident and Event Management (SIEM) software platform.
- The SIEM solution will be deployed by policy to all devices for all users after initial logon and deliver protection of all devices both used by users, delivered through the cloud and for services delivered through Microsoft Office 365.
- The SIEM will be installed on each device as an agent through policy and will not be removable by users.
- The SIEM will be installed as a "Enterprise App" into Microsoft Office 365 to deliver 365 cloud monitoring.
- Anomalies identified by the SIEM (unusual user / device activity, login issues, compromised credentials etc) will be triaged by the SOC team and they will alert the (Internal Service Desk / Director of Technology (James Reilly)) once the alert is verified and a confirmed threat.

VULNERABILITY SCANNING

- Assembly Global Networks will utilise the SIEM solution to deliver 12 hourly vulnerability assessments which will be monitored by the (Internal Helpdesk / (Director of Technology (James Reilly)) who will address any issues with a CVSS V3 Score equal to or more than 7.0 and will review other lower CVSS scores to determine actions required to further improve the safety of Assembly Global Networks systems.
- At least annually as part of Assembly Global Networks' own Cyber Essentials Plus assessment, an external party will complete an authenticated vulnerability assessment of all systems and external IP addresses in use for all "in scope" locations and assets.
- The results of any scans by the SIEM or external party will be reflected (where necessary) in Assembly Global Networks' Business Risk Assessment and Security Policies as appropriate.

END OF LIFE / DATA DESTRUCTION

Equipment reaching End-of-Life will be returned to the Director of Technology (James Reilly) where the hard disk will be wiped to DoD standards using DBAN (or ABAN for SSD's) before a decision is made to either reload the device and pass onto a recycling charity or disposing of the device through a WEEE provider.

For data stored in Assembly Global Networks Systems, our retention policy (listed within our DPIA) will be followed and data removed when it reaches its detailed end-of-life.

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com

As a digital company its unlikely that we will have any printed material or data, however, where documents and information are printed or arrive printed, these will be disposed of securely through shredding. Our staff, who handle sensitive information, which is in printed form, will be provided with a cross-cut shredder to ensure that disposal is secure. If you require shredding capabilities, please notify your line manager.

RESPONSE

INFORMATION SECURITY INCIDENTS

- All breaches of this policy and all other information security incidents shall be reported to the Director of Technology (James Reilly) and/or the Managing Director (Peter Smith)
- If required because of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Director of Technology (James Reilly) or Managing Director (Peter Smith)
- Information Security Incidents shall be recorded in the Security Incident Log and investigated by the Director of Technology (James Reilly) to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.
- The Managing Director (Peter Smith) shall decide whether any such incident is reportable to the authorities, such as the Information Commissioners Office (ICO) or other appropriate body.

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS

- Assembly Global Networks shall maintain a Business Continuity and Disaster Recovery Plan (Business Continuity Plan) for all mission critical systems, information assets, applications, and networks.
- The Business Continuity Plan will be reviewed at least annually by the Director of Technology (James Reilly)
- The Business Continuity Plan will be tested (walk through exercise) at least annually
- Generically, with all staff working 100% remotely on cloud systems, localised interruptions for staff are not company impacting; where deemed necessary, those staff requiring continual connectivity for delivery impacting situations, will have additional access methods, such as tethering of mobile phone for data access as well as a local internet connection.

REPORTING

- The Director of Technology (James Reilly) shall keep {company name} Board of Directors (and wider staff) up to date with information regarding the security status of Assembly Global Networks by means of regular reports to the board and where necessary wider staff.
- Any required external reporting of security incidents or information shall be authorised by the Managing Director (Peter Smith)

FURTHER INFORMATION

- Further information and guidance regarding this policy can be obtained from the Director of Technology (James Reilly)
- Comments and/or suggestions to help improve security are always welcome and can be sent at anytime to the Director of Technology (James Reilly), Managing Director (Peter Smith) or any other director.

Policy Approved by Peter Smith, Managing Director
30/06/2025

83 Victoria Street
London
SW1H 0HW
020 3795 6880
enquiries@assemblymanaged.com