Cyber Safety Policy 2024-26

Version 1.0
Date 28/04/2023
Review Date 28/04/2024

POLICY TITLE	Super Poly Ltd Information Security Policy

ISSUE DATE	April 2023	**REVIEW DATE**	August 2026

VERSION	1.0	**ISSUED BY**	Julian Ernst, Eddie Nixon and Sam Ernst (Directors)

ASSOCIATED DOCUMENTS	All policies of Super Poly Ltd.

APPROVED BY	Directors	**DATE**	{Approved Date}

REVIEW AND CONSULTATION PROCESS	This policy will be reviewed by the directors at least annually. Changes and amendments will be review by them and authorised for release at quarterly management meetings.

RESPONSIBILITY FOR IMPLEMENTATION AND TRAINING	Directors are 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	{when}	{who}	Initial Draft for review
0.2			Update post initial review
1.0	August 2023	Helen Ernst	Initial Release

DISTRIBUTION	This policy document will be made available to all staff in Super Poly Ltd. It will be stored in the shared drive- Business Management folder as Read-Only Version

Contents

INTRODUCTION

This Information Security Policy is a key component of Super Poly ltd.'s business management framework and is designed to set out the requirements and responsibilities for maintaining the security of information within the business.

It is expected that any data partners who are authorised to work Super Poly ltd will also comply with the requirements of this policy when dealing with Super Poly Ltd.

This policy is in relation to the systems utilised by Super Poly Ltd for the delivery of services to our customers and partners. Those not interacting or utilising Super Poly Ltd systems they will not be expected to adhere to this policy.

AIM AND SCOPE OF THIS POLICY

This policy sets out the rules governing the secure management of Super Poly Ltd.'s 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 security
- 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 applies to all information assets, data information systems, networks, applications, locations (both office, home office and mobile) and staff of Super Poly Ltd and/or contractors or services supplied under contract to Super Poly Ltd.

The policy is designed to be read as both our Information Security Policy as well as our generic acceptable use policy, which covers 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:

- Sage 200
- One Drive
- Corporate Website
- Microsoft Outlook (including Email, Teams)

- RESPONSIBILITIES

Ultimate responsibility for information security rests with the Directors of Super Poly Ltd, but on a day-to-day basis the management team shall be responsible for managing and implementing the policy and related procedures.

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

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 Super Poly Ltd.'s data. Failure to do so may result in disciplinary action.
- The management team shall be responsible for the security of information within the overall 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.

LEGISLATION

Super Poly Ltd is required to 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 Super Poly Ltd, who may be held personally accountable for any breaches of information security for which they are responsible.

Super Ply Ltd 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

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 during induction
- 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 induction 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

- Super Poly Ltd shall ensure that all software is properly licensed and approved by the directors.
- Individual and Super Poly Ltd 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 a pin or face recognition.
- Biometrics, including Windows Hello can be used by the underlying PIN/ facial recognition must apply

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 Directors as they are responsible for the security of the systems, they are the IAO’s (Information Asset Owners). The directors (IAO’s) are recorded in the company’s 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 Directors 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 Directors and they will ultimately decide about provision of access, ensuring there is a valid business case for the change to be made.
- The Directors are 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 being duly authorised.

ADMINISTRATIVE ACCESS

- Administrative access will only be provided to any person with Director approval.
- Like standard accounts, administrative accounts MUST utilise Multi-Factor Authentication, if available.
- Directors will review, at least annually, who has administrative access to their systems.
- All requests for administrative access are to be made by email to Directors for approval.
- 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.

ACCESS REVIEWS

- The management team will complete a review audit of the users who have access to the companies Information Assets. Yearly audits 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. Temporary, open connections will be removed as soon as possible after opening.

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.
- Super Poly Ltd 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 IT support services 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.*

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 Super Poly Ltd 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:

- 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 {Super Poly Ltd systems. The IT support services 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.

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. Super Poly Ltd 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.*

MONITORING SYSTEM ACCESS AND USE

- Where supported and available by the information system, a full audit trail will be recorded and reviewed yearly. Monitoring will generally be completed through our DPIA (data protection and information assessment)
- Super Poly ltd 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.
- Super Poly Ltd may 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 Super Poly Ltd Information Asset or any device accessing Super Poly Ltd.'s secure 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 this policy.
- Encrypted from boot/start up, for entire device and not just data areas.
- If a mobile, only access Super Poly Ltd systems using the secure routes created for an isolated work profile on the device which is controlled by Super Poly Ltd. This 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" Super Poly Ltd 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 our pin/ facial recognition system 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, and accept the required policies pushed out from Super Poly Ltd systems onto their device generating the Work Profile by installing the Company applications. Installation of the Company applications to access Company Data confirms your acceptance to the policy.

ASSET MANAGEMENT

ASSET OWNERSHIP

- The Directors of Super Poly Ltd will be the custodians of each individual asset (hardware, software, application, or data) and are 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.

ASSET HANDLING

ASSET CLASSIFICATION

- Super Poly Ltd 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
Customer ONLY	Information generated from our assessments and working with clients which is strictly confidential between Super Poly and the customer. The exception to Super Poly Ltd and the customer confidentiality is where we are working with a customer with a partner/contractor/agency, where the confidentiality chain exists between Super Poly Ltd, our/customers partners/contractor/agency and the end-customer.	• Project details / Project Information • Work requests • Contracts for the delivery of services • Commercial Agreements • Non-Disclosure Agreements • Service Level 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 • Customer Contact Details • Price lists • Company plans / financials • Employee Salary Information • Any data classed as "Sensitive personal data" under the Data Protection Act

		/ General Data Protection Regulations.

- Super Poly Ltd strives to be 100% electronic in terms of service delivery and management systems and therefore does 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.

ASSET CLASSIFICATION DATA SEGREGATION

- Super Poly Ltd 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 Super Poly Ltd and of course, “Customer” which cannot be shared with anyone except the customer and those staff internally who need to have access to the information.
    - Super Poly Ltd works with “Partners” for the delivery of services to their clients, therefore “customer” can be either the end-user or the “Partner/Contractor” who we are working with to deliver services to the end-client.

CATEGORY	SYSTEM	NOTES
PUBLIC SYSTEMS	**Super Poly Ltd Website**	**Content for general release will be stored in open access areas on the website**
Customer ONLY SYSTEMS	**Electronic Signature** **LinkedIn**	**Information stored within these systems should remain confidential and access to information for a customer should only be to their own information and only then if there is a requirement to provide that information.**
INTERNAL SYSTEMS	Sage 200 One Drive Microsoft Outlook	**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, maybe the use of teams or zoom which may link to external agents**

REMOVABLE MEDIA

In general, there is no requirement for the use of removable media for the storage or transport of any data.

In the unlikely need that removable media is required for data transit, (USB devices) employee's will seek the advice of the Directors to review the security requirements and risks around the required data set and its transportation.

PERSONAL DEVICES / BRING YOUR OWN DEVICE (BYOD)

Super Poly Ltd supports the use of Bring-Your-Own-Devices. BYOD will be used as “the normal” to include email access. However employee’s will be provided with company devices (laptops) to carry out their day-to-day business operations.

Any person using a BYOD device will be required to comply with the stringent policies required for any device being used to access Super Poly Ltd systems, these include but are not limited to:

- No shared accounts on the system
- Users who access company data on a mobile phone will understand that no unauthorised apps are to be used on the mobile device. We maintain a list of approved apps which can be used on mobile devices (see appendix 1)
- 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 Super Poly ltd 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 Super Poly Ltd patch management application to allow Super Poly Ltd to maintain patching on the device.
- Working from home on any BYOD device on Super Poly Ltd systems confirms your acceptance to this policy.

Super Poly Ltd 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.

SOCIAL MEDIA

- Personal Social Media may only be used outside of business hours. 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 Directors.

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 Directors.

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 Directors or an outsourced IT service provider.

SYSTEMS CHANGE CONTROL

- Any information system requiring a change will be subject to risk assessment and processed through the Super Poly Ltd Change Management Process (see additional procedural documents.
    - 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

- Super Poly Ltd 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 Super Poly Ltd as relevant at the time.
- Systems will be correctly sized, designed with security first in mind and changes approved by the Directors 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 Super Poly Ltd Patch Management System. The IT Support provider use a patch management software to automate updates on all laptops & desktops. All Critical & Security updates are installed on a weekly basis. We also process service pack updates, Office updates, Java updates, and Adobe updates through the same software.
- 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.
- Users shall not install any software or other active code onto their devices without the express permission of the Directors, utilising the Change Management Procedure. (Installation of any unauthorised applications will be blocked by the Super Poly Ltd,
- 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.
- Super Poly Ltd will utilise a 3rd Party Backup solution (Datto SaaS) to protect the information assets stored within Microsoft 365 to ensure we have longer backup protection windows than that afforded by Microsoft.

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

- Super Poly Ltd will utilise Avast Cloud Care as our anti-virus technology to align to the current UK Cyber Security Standards. This will be centrally administered, and users will not have the ability to prevent its operation.

END OF LIFE / DATA DESTRUCTION

Equipment reaching End-of-Life will be returned to the Directors where the hard disk will be wiped to DoD standards using DBAN 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 Super Poly Ltd.'s Systems, our retention policy (listed within our DPIA) will be followed and data removed when it reaches its detailed end-of-life.

As a digital company it's 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 Directors.
- If required because of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Directors.
- Information Security Incidents shall be recorded in the non-conformance log and investigated by the Directors 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 Directors 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

- Super Poly Ltd shall maintain a Business Risks and Opportunities Register for all mission critical systems, information assets, applications, and networks.
- The Risks and Opportunities Plan will be reviewed at least annually by the Directors.
- The Risks and Opportunities 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 Directors shall keep Super Poly Ltd.'s wider staff up to date with information regarding the security status of Super Poly Ltd by means of regular reports where necessary to them
- Any required external reporting of security incidents or information shall be authorised by the Directors.

FURTHER INFORMATION

- Further information and guidance regarding this policy can be obtained from the Directors.
- Comments and/or suggestions to help improve security are always welcome and can be sent at any time to the Directors.

Policy Approved by
Sam Ernst
September 2023

APPENDIX 1
APPROVED APPS LIST

Financial
Banking apps
Credit card apps
Paypal
Wallet
Insurance/Life policy apps

Productivity
Email
Authentication
Contacts
Reminders
Files
Acrobat
Notes
Zoom

Information and Reading
Audio Books/Kindle
Weather
BBC News
Newspaper apps

Social Media
Facebook
Tick Tock
Instagram
Whatsapp
Linked-In
Messaging

Utilities
Car apps
Apps Store
Doorbell 'Ring'
Mobile provider apps
Find My Iphone
Clock
Calculator
Apple Watch
Google
Energy provider apps

Shopping and Food
Supermarket Apps
Clothing Apps
Amazon
Ebay
Moonpig
Store rewards apps
Deliveroo
Just Eat

Entertainment
Football apps
TV channels
YouTube
Shazam
Radio stations
Music apps

Health and Fitness
Gym members apps
Healthcare apps
NHS app
Apple Watch fitness app

Navigation
Google maps
Waze

Travel
Taxi firm apps
Trainline
Metrolink
Airport apps
Car parking apps

Games
Scrabble
Word games
Solitaire
Soduko