ACCESS CONTROL POLICY

1 – Policy Overview

1.1 – Policy Scope

This policy applies to:

- All Projecting Success employees.
- Any user accessing Projecting Success's confidential information.

2 – Access Control

To be able to uniquely identify and track each user for the purpose of access control to all networks, systems, and applications that contain Confidential Information Projecting Success must comply with the measures outlined in this Policy.

There will be 3 levels of access:

1. **0365 access.** Employees or trusted 3rd parties who are provided with an O365 account. They will have access to all of SharePoint in accordance with the access control policy.
2. **Limited access.** This will be applied on a case-by-case basis but will generally apply to interns working with the company or 3rd parties. Access will be granted to specific ring-fenced folders which will be segregated from the main filing structure.
3. **Per file or folder access.** Access will be granted to access or edit specific files or folders, where individuals are provided with access to the file rather than forwarding the file via email.

2.1 – Share Point

- When requesting access to SharePoint the user must supply their assigned unique user identification in conjunction with a secure password to gain access.
- Each user's password should comply with the Projecting Success password policy.
- Users must not allow another user to use their unique user identification or password.
- Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner.

- Each user must ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications.

- 3rd Parties will be confined to Projecting Success' SharePoint extranet where they will only have access to their named folder with enclosed information that is relevant to them and Projecting Success. This does not apply to joint initiatives which are core to Projecting Success' Services.

    - In instances where 3rd parties are collaborating with Projecting Success on joint initiatives that are of high significance to business objectives and are ongoing, a dedicated SharePoint site will be created on the Projecting Success Intranet. These sites will have access restrictions similar to traditional SharePoint sites. These initiatives are listed below with justification as to why they are not suitable to be managed via the extranet:

        - Construction Data Trust: Projecting Success are the appointed stewards, lead for technical implementation of the data trust platform, host of the trust and communications platform and are project managing mobilisation. Due to the levels of responsibility, an extranet set of folders would not be sufficient for collaboration across multiple organisations.

        - Project Data Analytics Task Force (PDATF): The PDATF is a join initiative across eight plus organisations. Projecting Success Co-chair the PDATF. Due to the dynamic nature of the PDATF and its members, managing access via extranet is not feasible. Particularly as collaboration requires a teams environment for secure communication. This environment needs to be tied to a site which does not fit the scope of the extranet. A dedicated SharePoint will allow for easier management and restriction of access.

2.2 - Personal Devices

- Projecting Success are certified in cyber essentials and therefore all devices used to access the Projecting Success Microsoft tenant will require two-factor authentication.

- Employees will be allowed to access confidential information on personal devices, but this will be restricted when working overseas. By default, work resources are inaccessible when

operating overseas. Restrictions can be lessened for critical business purposed but this requires approval from senior leadership team and ISM leads.

- Devices must be password protected by a password compliant with the Projecting Success password policy and also requirements set by cyber essentials certification.
- An inactivity timer, that will terminate the user session and lock the device, of maximum 15 minutes must be applied to all devices.
- When leaving a device Users must lock or activate the systems automatic logoff mechanism or logout of all applications containing Confidential Information.
- Windows laptops will need to have Windows Defender Firewall and virus check active with a virus check occurring monthly, anything found must be removed straight away.
- Mac users must ensure that FileVault and Firewall is turned on. Default anti-malware software will be suitable.
- Default anti-malware for mobile phones will be suitable.
- Only install trusted applications onto a device containing sensitive information.
- No documents may be left unattended, desks must always be kept clear to ensure that no confidential information is lost or compromised.
- Bit locker protection must be used for all compatible windows systems.
- Mobile devices are required to be up-to-date at all times and need to be encrypted with a strong passcode and/or biometrics.

2.3 – Further Controls

- Projecting Success shall implement the controls specified within the O365 security roadmap. Any exceptions to this, such as where a O365 policy results in a software incompatibility with Mac, shall be agreed with the CEO.
- Alert policies shall be established that to provide alerts when specific conditions have been reached, such as malware activity or data loss incidents.

- IT support shall conduct a 100% annual audit with all members of staff to ensure that virus and malware protection is appropriately configured, access controls are set up (including firewalls), all drives are encrypted and that all software is regularly patched.
- Implementation of cyber essentials to further prevent breaches and potential compromise of security system.
- Intune is used to remove bloatware during enrolment process. Only applications from Intune can be installed on PC's or if given permission from IT admin, may install other approved software on a case-by-case basis. This will prevent access to any unauthorised areas/software.

2.4 – Penetration Testing

Penetration testing is conducted on the company 0365 domain annually. Reports can be found here. However, it is worth noting that Projecting Success does not operate a company network. It does not operate its own servers. The majority of its data assets are in the cloud, with the remainder stored on encrypted drives or in locked filing cabinets. The O365 cloud can be accessed via anyone, therefore, we rely on O365 security features to protect our assets. However, this doesn't resolve the risk completely. The residual risks are:

2.4.1 – Man in the Middle Attacks

This is particularly relevant when staff are using public Wi-Fi. All staff are aware of the potential risks and have been trained to consider what data they are passing through public Wi-Fi networks to minimise any risk to the business. For instance, the company will not action any financial transactions using public networks.

2.4.2 – Compromised Assets

There is also a risk that assets used by staff are compromised. We mitigate this risk through the 100% audit, to ensure that assets are appropriately configured.

2.5 – Information Security Events

In the case of a breach, depending on the severity, the Information Security Manager will be notified through either email or Phone call.

2.6 – Data Protection

The data protection policy is defined in the staff handbook.

2.7 – Computer Misuse

The conditions relating to computer misuse are defined in the internet and email section of the staff handbook.

2.8 – Confidentiality

All staff are subject to confidentiality agreements. The conditions pertaining to this are defined in the member of staff's contract of employment.

2.9 – Roles and Responsibilities

All staff have been trained to ensure compliance with the appropriate controls.

2.10 – Compliance

Projecting Success management will carry out checks on all employee's every 6 months to ensure they are complying with the policy. Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

Version History				
Date	Version	Details of Change	Revision By	QA
28/08/2018	1	- Document Created.	George Davies	Martin Paver
31/08/2018	2	- Added policy to ensure physical documents are not left unattended.	George Davies	Martin Paver
14/10/2018	3	- Added Bit Locker protection for windows devices.	George Davies	Martin Paver
15/10/2018	4	- Updates following ISO27001 audit.	Martin Paver	Martin Paver
15/10/2019	5	- Annual Review.	George Davies	Martin Paver
04/11/2019	6	- Updated wording for BitLocker controls as it is not compatible with all windows versions.	George Davies	Martin Paver
08/10/2020	7	- Annual Review.	Martin Paver	Martin Paver
28/04/2020	8	- Implemented access controls for those working in teams groups / planners which includes internal members and guests.	Yoshi Soornack	Martin Paver
03/08/2021	9	- Included the implementation of cyber essentials.	Yoshi Soornack	Martin Paver
21/09/2021	10	- Alteration to 3rd parties' access, due to deeper involvement on joint initiatives. 3rd parties are not exclusively confined to extranet in specific cases.	Yoshi Soornack	Martin Paver

22/06/2022	11	- Added information to reflect cyber essentials updates.	Jake Bennet	Yoshi Soornack
23/08/2022	12	- Expanded staff training to whole organisation, implementation of penetration testing procedures annually.	Yoshi Soornack