[Your Company Name]

Access Control & Password Policy

DOCUMENT AUTHOR:	[Insert Author]
DOCUMENT OWNER:	[Insert Owner]
STATUS:	[Draft/Approved]
DATE CREATED:	[Insert Date]
VERSION:	[Insert Version]
LAST UPDATED:	[Insert Date]
SECURITY CLASSIFICATION:	[High/Medium/Low]

Document Customisation

This page *(to end of the 'disclaimer')* provides template guidance and ***must be removed*** from the finished version. For information on customising this template, please refer to the *'Instructions'* supplied with your order.

It is important to work through the document and customise any areas to ensure that the finished template accurately reflects what your organisation does and the controls that you have in place. You should consider your regulatory and legal obligations and any standards or requirements that apply to your industry or business type when customising the content.

Template Guidance

We have provided a generic template as a starting point for you to develop your own document in this compliance area. You should review and customise the template sections thoroughly to ensure that the finished version accurately reflects your organisations' controls and responsibilities.

This template has been developed to compliment the Know Your Compliance Limited Information Security Pack and should be used in conjunction with the other documents in the pack. The pack is a generic suite of policies designed to help firms meet the requirements of information security.

The templates in our IS pack cover some of the areas specified in Cyber Essentials and ISO27001 but are not a complete solution for these certifications as they do not cover all of the standards and requirements. If using our IS pack for a certification program, you must ensure that you develop your own policies and cover each of the mandatory areas within the relevant standard.

Referencing Other Policies

We sometimes reference other policies in a template where relevant *(i.e. refer to Anti-Bribery & Corruption Policy in conjunction with AML).* Referenced documents are **only** included in your pack if you have ordered them separately or you have purchased a Toolkit or Bundle that includes them.

Licence Terms

Purchased documents are for use within the ordering company **only** and cannot be used, sold or transferred elsewhere without written permission from Know Your Compliance Limited. Please refer to the *'Instructions'* document for more information on our T&C's and licence options.

Disclaimer

Know Your Compliance Limited has created this template for you to use in developing and implementing your compliance program requirements. Whilst every reasonable care is taken to ensure that the content is relevant, compliant and up to date; it is **your responsibility** to ensure that the finished policy complies with any regulatory and/or legal requirements and standards.

It is important that you customise the content to suit your industry needs and business type. Know Your Compliance Limited makes no claims or guarantees about the compliance or adequacy of the template content and accepts no responsibility or liability for any loss, damage or expense incurred as a result of reliance on our documents. If you are unsure of your obligations, you should obtain legal or professional advice before publishing, using or relying upon your finished policy.

Revision History

VERSION	REVISION DATE	SECTION REVISED	REASON FOR REVISION	DESCRIPTION OF REVISION

Table of Contents

1 Policy Statement 5
2 Purpose 5
3 Scope 5
4 Objectives 6
5 Procedures, Controls and Measures 6
5.1 Logical Access Control 7
5.1.1 Role-Based Access 7
5.1.2 Manager Access 7
5.1.3 Individual Access 7
5.2 Passwords 8
5.2.1 Password Creation & Change 8
5.2.2 Default Passwords 9
5.2.3 Protecting Passwords 9
5.3 User ID's and Badges 10
5.4 Privileged Accounts 10
5.5 Authorised Access 10
5.5.1 Login Controls 10
5.5.2 Credentials & Roles 11
5.6 Physical Access Controls 11
5.6.1 Door & Window Controls 11
5.6.2 Outside Opening Hours 11
5.6.3 Direct Access 12
5.7 Leavers & End of Contract 12
6 Responsibilities 12

1 POLICY STATEMENT

It is **[Your Company Name]'s** *(hereinafter referred to as the **"Company"**)* policy to protect and secure the information and systems within our remit and we take this function very seriously. We have developed and implemented several physical, logical and procedural measures and controls to enforce our approach. We understand that it is vital to protect the systems and information held and used by us from unauthorised use or access and are fully aware of how such access can affect security, personal information and individuals. ***The types of measures and controls used by The Company are: -***

- [illegible]
- [illegible]
- [illegible]

2 PURPOSE

The purpose of this policy is to ensure that system based and physical access to any information, location and/or system is controlled and where applicable restricted using controls and procedures that protect the associated information systems and data. The Company is committed to the security of the information and assets within our remit and enforce and stress test all access measures to ensure their functionality, effectiveness and purpose.

This Access Control & Password Policy aims to restrict access to controlled information and/or systems to only those staff or third parties who are authorised or have written permission from the Company. Where temporary and/or partial access to information or systems is required, we follow strict protocols to only enable access to the information or for the duration required by the activity.

3 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

Page removed from sample document

5.1 LOGICAL ACCESS CONTROL

Access to systems within the Company are governed by our based logical access control measures. Access to any system is classified as one of the below access levels and restrictions are implemented at the user level. Levels can be changed at the discretion of the **[designated person/IT Manager]** and pending completion of an access change form. **Considerations for granting access is assessed based on:-**

- An employee or user's need of access to complete their job and/or task
- Duration of access
- Level of access
- Information types located on the system in questions
- Security measures in place if access is granted
- Ability to remove access at a predetermined time
- Access is tackled and allocated on a case by case basis and can only be assigned by the **[designated person/IT Manager]**.

5.1.1 ROLE-BASED ACCESS

Users are identified as being part of a group (such as employee) and their level of access is granted to all required areas. This level of access is inherited by all group members and is controlled by the **[designated person/IT Manager]**. Such group access is considered necessary for each employee to enable them to carry out their job and includes access to areas such as email, printers, the Company collection system and phone system. Directors, the **[designated person/IT Manager]** and Managerial staff can assign role-based access.

5.1.2 MANAGER ACCESS

System access is granted at a higher level for managers and Directors who can access more system areas than generic employees. Such access is deemed essential to their oversight role and enables managerial staff to carry out functions and processes that require access to personal information, secure systems or data. Manager access is not inherited by the group and only the **[designated person/IT Manager]** can assign Manager Access.

5.1.3 INDIVIDUAL ACCESS

System access is granted at the required level based on a business and/or legal requirement and is only granted to the individual(s) who requires access (*i.e. if an employee is granted extended access, this is not inherited by any other role-based group member*). Individual access is usually granted for a limited period by the **[designated person/IT Manager]** and is deactivated after the set period. Such access may include a role-based user needing access to sensitive information or restricted systems to perform a task or one-off project.

5.2 PASSWORDS

Passwords are a key part of the Company's protection strategy and are used throughout the company to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third parties who are responsible for one or more account, system or have access to any resource that requires a password.

5.2.1 PASSWORD CREATION & CHANGE

[illegible]

[illegible]

Strong passwords are enforced on systems and by users and must be: -

- More than 8 characters
- Include letters, numbers and at least 1 special characters
- Not be easily recognisable *(i.e. no names, dates of birth, places etc*)
- Must include upper and lowercase letters
- **[Add/delete as applicable]**

All passwords are changed monthly, and users are not permitted to reuse the same password within a 3-month period. This is forced using software on all systems and a password change is automatically promoted at the start of each month. This change is enforced within **[insert number of days]** of the change reminder being shown.

If a password is forgotten, only the [**designated person/IT Manager**] can reset passwords. Passwords that have been forgotten are changed by default and cannot be reset with a previously used password. A forced change of password is required where a user knows or suspects that their password or system may have been compromised.

Page removed from sample document

5.3 User ID's and Badges

[Delete if not applicable]

The Company has adopted ID badges for all employees, visitors and third parties who are in our office building. Such badges are specific to those they are assigned to and ID's or badges not in use are stored in a secure, locked area.

[illegible]

[illegible]

5.4 Privileged Accounts

[illegible]

5.5 Authorised Access

The Company keeps an Access Register and details which employees or third parties have access to which systems and information. The register also notes when the access was given, when it will be restricted (*if temporary access*), the type of data or system being accessed and the reason for access.

5.5.1 Login Controls

Systems can only be accessed by secure authentication of user validation, which consists of a username and password at the role-based user level. All computers have an active firewall and default to a lock screen with user authentication required after **[1/2/5/10/15]** minutes of inactivity. All staff are aware that if they leave their workstation, their monitor is to be turned off and their

system locked. All computers are closed down at the end of the day and are not allowed to be left running out of business hours.

5.5.2 CREDENTIALS & ROLES

[illegible]

[illegible]

5.6 PHYSICAL ACCESS CONTROLS

[illegible]

5.6.1 DOOR & WINDOW CONTROLS

The Company has **[insert number & location of entrance/exit points]** providing access to the building/office, which are secured via **[insert security measures (i.e. deadbolts, CCTV, alarms, biometrics etc).]**

All windows are alarmed and are kept locked when the building is vacated. Windows open during the day are secured with restricted access hinges to prevent access. Visitors are escorted at all times during a visit and are given an ID badge. They are also required to sign in and out in our access register and sign a confidentiality agreement. Where a visitor is required to carry any bag with them (*including laptops*), we reserve the right to search them on entering and leaving the building.
Outside Opening Hours

When the building has been vacated at the end of working hours, the alarm system is activated and secures all windows and doors. The building is *'locked down'* after **[18:00]** and any alarm trigger will immediately notify the **[director/manager/police/security services]** who have a contact tree for the Director and deputy. **[Insert out of hours alarm protocols]**

Page removed from sample document