Access Control Policy

Document Ref.	**GDPR-DOC-10-3**
Version:	**1**
Dated:	**16 May 2018**
Document Author:	**Steve Brown**
Document Owner:	**Steve Brown**

Revision History

Version	Date	Revision Author	Summary of Changes
1	16/05/2018	Steve Brown	

Distribution

Name	Title
Public	Available via website

Approval

Name	Position	Signature	Date
Steve Brown	GDPR / Data Protection Officer		15/05/2018

Contents

1 Introduction

The control of access to our information assets is a fundamental part of a defence in depth strategy to information security. If we are to effectively protect the confidentiality, integrity and availability of classified data then we must ensure that a comprehensive mix of physical and logical controls are in place.

But our policy with regard to access control must ensure that the measures we implement are appropriate to the business requirement for protection and are not unnecessarily strict. The policy therefore must be based upon a clear understanding of the business requirements as specified by the owners of the assets involved.

These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service
- Relevant legislation that may apply e.g. the GDPR, Sarbanes Oxley
- The regulatory framework in which the organization and the system operates
- Contractual obligations to external third parties
- The threats, vulnerabilities and risks involved
- The organization's appetite for risk

This access control policy is designed to take account of the business and information security requirements of the organization and is subject to regular review to ensure that it remains appropriate.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Ipswich Rugby Football Club Limited systems.

The following policies and procedures are relevant to this document:

- *Cloud Computing Policy*

2 Business Requirements of Access Control

Business requirements for access control must be established as part of the requirements-gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design.

Information security requirements must be clearly stated within the business requirements specification document and must take account of the organization's standards.

In addition to the specific requirements, a number of general principles will be used when designing access controls for Ipswich Rugby Football Club Limited systems and services.

These are:

- ***Defence in Depth*** – security must not depend upon any single control but be the sum of a number of complementary controls
- ***Least Privilege*** – the default approach taken must be to assume that access is not required, rather than to assume that it is
- ***Need to Know*** – access is only granted to the information required to perform a role, and no more
- ***Need to Use*** – Users will only be able to access physical and logical facilities required for their role

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities and therefore the number and severity of security incidents that occur.

As part of the selection of cloud service providers specifically, the following access-related considerations must be taken into account:

- User registration and deregistration functions provided
- Facilities for managing access rights to the cloud service
- To what extent access to cloud services, cloud service functions and cloud service customer data can be controlled on an as required basis
- Availability of multi-factor authentication for administrator accounts
- Procedures for the allocation of secret information such as passwords

Addressing these requirements as part of the selection process will ensure that the provisions of this policy can be met in the cloud as well as within on-premise systems.

3 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

3.1 User Registration and Deregistration

A request for access to the organization's network and computer systems must first be submitted to the System Administrator for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorisation is obtained prior to user account creation. The principle of segregation of duties will apply so that the creation of the user account and the assignment of permissions are performed by different people.

Each user account will have a unique user name that is not shared with any other user and is associated with a specific individual i.e. not a role or job title. Generic user accounts i.e. single accounts to be used by a group of people must not be created as they provide insufficient allocation of responsibility.

An initial strong password must be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account.

When an employee leaves the organization under normal circumstances, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the System Administrator.

In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm the organization prior to or upon termination, a request to remove access may be approved and actioned in advance of notice of termination being given. This precaution will especially apply in the case where the individual concerned has privileged access rights e.g. domain admin.

User accounts must be initially suspended or disabled only and not deleted. User account names must not be reused as this may cause confusion in the event of a later investigation.

3.2 User Access Provisioning

Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general, this will be role-based i.e. a user account will be added to a group that has been created with the access permissions required by that job role.

Group roles must be maintained in line with business requirements and any changes to them must be formally authorised and controlled via the change management process.

Ad-hoc additional permissions must not be granted to user accounts outside of the group role; if such permissions are required this must be addressed as a change and formally requested.

3.3 Removal or Adjustment of Access Rights

Where an adjustment of access rights or permissions is required e.g. due to an individual changing role, this must be carried out as part of the role change. It must be ensured that access rights no longer required as part of the new role are removed from the user account. In the event that a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role must be requested via change management. Due consideration of any issues of segregation of duties must be given.

Under no circumstances will administrators be permitted to change their own user accounts or permissions.

3.4 Management of Privileged Access Rights

Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled. In general, technical users (such as IT support staff) will not make day to day use of user accounts with privileged access, rather a separate “admin” user account must be created and used only when the additional privileges are required. These accounts must be specific to an individual e.g. “John Smith Admin”; generic admin accounts must not be used as they provide insufficient identification of the user.

Access to admin level permissions must only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

The use of user accounts with privileged access in automated routines such as batch or interface jobs must be avoided where possible. Where this is unavoidable the password used must be protected and changed on a regular basis.

3.5 User Authentication for External Connections

In line with the *Network Security Policy* the use of modems on non-organization owned PCs or devices connected to the organization's network can seriously compromise the security of the network. Specific approval must be obtained from the System Administrator before connecting any equipment to the organization's network.

Where remote access to the network is required via VPN, a request must be made via the System Administrator. A policy of using two factor authentication for remote access will be used in line with the principle of "something you have and something you know" in order to reduce the risk of unauthorised access from the Internet.

For further information please refer to the *Mobile Device Policy*.

3.6 Supplier Remote Access to the Organization Network

Partner agencies or 3rd party suppliers must not be given details of how to access the organization's network without permission from the System Administrator. Any changes to supplier's connections (e.g. on termination of a contract) must be immediately sent to the System Administrator so that access can be updated or ceased. All permissions and access methods must be controlled by the System Administrator.

Partners or 3rd party suppliers must contact the System Administrator on each occasion to request permission to connect to the network and a log of activity must be maintained. Remote access software and user accounts must be disabled when not in use.

3.7 Review of User Access Rights

On a regular basis (at least annually) asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. This will be to identify:

- People who should not have access (e.g. leavers)
- User accounts with more access than required by the role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification e.g. generic or shared accounts
- Any other issues that do not comply with this policy

This review will be performed according to a formal procedure and any corrective actions identified and carried out.

A review of user accounts with privileged access will be carried out by the System Administrator on a quarterly basis to ensure that this policy is being complied with.

3.8 User Authentication and Password Policy

A strong password is an essential barrier against unauthorised access. Unfortunately, this area is often proven to be the weak link in an organization's security strategy and a variety of ways to improve the security of user authentication are available, including various forms of two factor authentication and biometric techniques.

Ipswich Rugby Football Club Limited's policy is to make use of additional authentication methods based on a risk assessment which takes into account:

- The value of the assets protected
- The degree of threat believed to exist
- The cost of the additional authentication method(s)
- The ease of use and practicality of the proposed method(s)
- Any other relevant controls in place

Use of multi-factor authentication methods must be justified on the basis of the above factors and securely implemented and maintained where appropriate.

Single Sign-On (SSO) will be used within the internal network where supported by relevant systems unless the security requirements are deemed to be such that a further logon is required.

Whether single or multi-factor authentication is used, the quality of user passwords must be enforced in all networks and systems using the following parameters:

Parameter	Value
Minimum length	8
Maximum length	16
Re-use cycle	Cannot be the same as any of the previous 32 passwords
Characters Required	At least one capital letter At least one number
Password similarity	New password cannot contain username
Change Frequency	Every 365 days
Account lockout	On 5 incorrect logon attempts
Account lockout action	Account must be re-enabled by System Administrator
Other controls	Password cannot contain the user name

Any exceptions to these rules must be authorised by the System Administrator.

4 User Responsibilities

In order to exercise due care and try to ensure the security of its information, Ipswich Rugby Football Club Limited expends a significant amount of time and money in implementing effective controls to lessen risk and reduce vulnerabilities. However, much still depends upon the degree of care exercised by the users of networks and systems in their day to day roles. Many recent high-profile security breaches have been largely caused by unauthorised access to user accounts resulting from passwords being stolen or guessed.

It is vital therefore that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organization.

In order to maximise the security of our information every user must:

- Use a strong password i.e. one which is in line with the rules set out in this policy
- Never tell anyone their password or allow anyone else to use their account
- Not record the password in writing or electronically e.g. in a file or email
- Avoid using the same password for other user accounts, either personal or business-related
- Ensure that any PC or device they leave unattended connected to the network is locked or logged out
- Leave nothing on display that may contain access information such as login names and passwords
- Inform the System Administrator of any changes to their role and access requirements

Failure to comply with these requirements may result in the organization taking disciplinary action against the individual(s) concerned.

5 System and Application Access Control

As part of the evaluation process for new or significantly changed systems, requirements for effective access control must be addressed and appropriate measures implemented.

These must consist of a comprehensive security model that includes support for the following:

- Creation of individual user accounts
- Definition of roles or groups to which user accounts can be assigned
- Allocation of permissions to objects (e.g. files, programs, menus) of different types (e.g. read, write, delete, execute) to subjects (user accounts and groups)
- Provision of varying views of menu options and data according to the user account and its permission levels
- User account administration, including ability to disable and delete accounts
- User logon controls such as
    - Non-display of password as it is entered
    - Account lockout once number of incorrect logon attempts exceeds a specified threshold
    - Provide information about number of unsuccessful logon attempts and last successful logon once user has successfully logged on
    - Date and time-based logon restrictions
    - Device and location logon restrictions
- User inactivity timeout
- Password management, including
    - Ability for user to change password
    - Controls over acceptable passwords
    - Password expiry
    - Hashed/encrypted password storage and transmission
- Security auditing facilities, including logon/logoffs, unsuccessful logon attempts, object access and account administration activities

Where bespoke software development is undertaken, program source code must be protected from unauthorized access.

Access to utility programs that provide a method of bypassing system security (e.g. data manipulation tools) must be strictly controlled and their use restricted to identified individuals and specific circumstances e.g. as part of a named project or change.