|  |
| --- |
| **QUICKCOVER INSURANCE**  **ISP-AC-A01**  **[Internal]** |

|  |
| --- |
| **Access Control Policy** |

|  |
| --- |
| **Version 1**  **12th JULY 2023** |

**Document Reference**

|  |  |
| --- | --- |
| **Document Code:** | ISP-AC-A01 |
| **Document title:** | Access Control Policy |
| **Filename:** | ISP-AC-A01 Access Control Policy |
| **Author:** | Consultant |
| Owner: | QuickCover Insurance |
| **Date:** | 12th July 2023 |
| **Version:** | 1.0 |
| **Status:** | Draft |

**Revision Record**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Summary of Changes** | **Revision Author** |
| 1.0 Draft 1 | 12th July 2023 | Establishment of Access Control Policy | Consultant |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
| Jared Leto | Owner/Manager |
| Emily Dickenson | Secretary/Administrative Assistant |
|  |  |
|  |  |
| All Staff | All Staff |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
| Jared Leto | Chairman |  |  |

**Contents**

1. **Introduction 4**
2. **Business Requirements of Access Control 5**
3. **Personnel Access Management 6**
   1. Personnel Registration and Deregistration 6
   2. Personnel Access Provisioning 8
   3. Removal or Adjustment of Access Rights 8
   4. Management of Privileged Access Rights 8
   5. Personnel Authentication for External Connections 9
   6. Supplier Remote Access to the Organization Network 9
   7. Review of Personnel Access Rights 9
   8. Personnel Authentication and Password Policy 10
4. **Personnel Responsibilities 12**
5. **System and Application Access Control 13**
6. **Introduction**
   1. The control of access to QuickCover Insurance’s information assets is a fundamental part of a defense 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.
   2. 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.
   3. 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 Data Protection Act.
* 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
  1. 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.
  2. This control applies to all systems, people and processes that constitute the organization’s information systems, including Owners, Managers, staff, suppliers and other third parties who have access organization systems.
  3. The following policies and procedures are relevant to this document:
* *Mobile Device Policy*
* *Teleworking Policy*
* *Network Security Policy*
* *Internet Acceptable Use Policy*
* *Vendor Information Security Evaluation Process*

1. **Business Requirements of Access Control**
   1. 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.
   2. Information security requirements must be clearly stated within the business requirements specification document .
   3. A number of general principles will be used when designing access controls for Organization systems and services.
   4. These are:

* ***Defense 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*** – Personnel will only be able to access physical and logical facilities required for their role.
  1. 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.

1. **Personnel Access Management**

* Formal Personnel access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorized Personnel access and to prevent unauthorized access. They must cover all stages of the lifecycle of Personnel access, from the initial registration of new Personnel to the final deregistration of Personnel who no longer require access.
* Personnel 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 Personnel that are required to perform system administration tasks.

## Personnel Registration and Deregistration

* + 1. A request for access to the organization’s network and computer systems must first be submitted to the Manager/Owner for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorization is obtained prior to Personnel account creation. The principle of segregation of duties will apply so that the creation of the Personnel account and the assignment of permissions are performed by different personnel.
    2. Each Personnel account will have a unique Personnel name that is not shared with any other Personnel and is associated with a specific individual i.e. not a role or job title. Generic Personnel accounts i.e. single accounts to be used by a group of people must not be created as they provide insufficient allocation of responsibility.
    3. An initial strong password must be created on account setup and communicated to the Personnel via secure means. The Personnel must be required to change the password on first use of the account.
    4. When a personnel leaves the organization under normal circumstances, their access to computer systems, mobile devices and data must be suspended at the close of business on the personnel’s last working day. It is the responsibility of the Human Resources officer to request the suspension of the access rights via the Information Technology Officer /Manager.
    5. In exceptional circumstances where there is perceived to be a risk that the staff 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.
    6. Personnel accounts must be initially suspended or disabled only and not deleted. Personnel account names must not be reused as this may cause confusion in the event of a later investigation.

## Personnel Access Provisioning

* + 1. Each Personnel must be allocated access rights and permissions to computer systems and data that are corresponding with the tasks they are expected to perform. In general, this will be role-based i.e. a Personnel account will be added to a group that has been created with the access permissions required by that job role.
    2. Group roles must be maintained in line with business requirements and any changes to them must be formally authorized and controlled via the change management process.
    3. Impromptu additional permissions must not be granted to Personnel accounts outside of the group role; if such permissions are required this must be addressed as a change and formal request.

## Removal or Adjustment of Access Rights

* + 1. 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 Personnel account. In the event that a Personnel is taking on a new role in addition to their existing one then a new composite role must be requested via change management. Due consideration of any issues of segregation of duties must be given.
    2. Under no circumstances will administrators be permitted to change their own Personnel accounts or permissions.

## Management of Privileged Access Rights

* + 1. 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 Personnel will not make day to day use of Personnel accounts with privileged access, rather a separate “admin” Personnel 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 Personnel.
    2. 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.
    3. The use of Personnel 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.

## Personnel Authentication for External Connections

* + 1. 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 Manager/Owner before connecting any equipment to QuickCover Insurance’s network.
    2. Where remote access to the network is required via VPN, a request must be made via the Manager/Owner. 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 unauthorized access from the Internet.

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

## Supplier Remote Access to the Organization Network

* + 1. Partner agencies or 3rd party suppliers/vendors must not be given details of how to access the QuickCover Insurance’s network without permission from the Manager/Owner /Information Technology Officer. Any changes to supplier’s connections (e.g. on termination of a contract) must be immediately sent to the Information Technology Officer so that access can be updated or ceased. All permissions and access methods must be controlled by the Information Technology Officer.
    2. Partners or 3rd party suppliers /vendors must contact the Information Technology Officer on each occasion to request permission to connect to the network and a log of activity must be maintained. Remote access software and Personnel accounts must be disabled when not in use.

## Review of Personnel Access Rights

On a regular basis (at least bi-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:

* Personnel who must not have access (e.g. leavers)
* Personnel accounts with more access than required by the role
* Personnel accounts with incorrect role allocations
* Personnel accounts that do not provide adequate identification e.g. generic or shared accounts
* Any other issues that do not comply with this policy
  + 1. This review will be performed according to a formal procedure and any corrective actions identified and carried out.
    2. A review of Personnel accounts with privileged access will be carried out by the Manager/Owner/Auditor on a quarterly basis to ensure that this policy is being complied with.

## Personnel Authentication and Password Policy

* + 1. A strong password is an essential barrier against unauthorized 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 Personnel authentication are available, including various forms of two factor authentication and biometric techniques.
    2. Organization’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
  + 1. Use of multi-factor authentication methods must be justified on the basis of the above factors and securely implemented and maintained where appropriate.
    2. Single Sign-On (SSO) must not be used within the internal network.
    3. Whether single or multi-factor authentication is used, the quality of Personnel 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 passwords |
| Characters Required | At least one capital letter  At least one symbol  At least one number |
| Password similarity | New password cannot share more than three characters in the same position as the old password |
| Change Frequency | At least every 60 days |
| Account lockout | On 3 incorrect logon attempts |
| Account lockout action | Account must be re-enabled by Information Technology Officer upon official request by the account owner. |
| Other controls | Password cannot contain the Personnel name |

* + 1. Any exceptions to these rules must be authorized by the Manager/Owner.

1. **Personnel Responsibilities**
   1. In order to exercise due care and try to ensure the security of its information, Organization 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 Personnel of networks and systems in their day to day roles. Many recent high-profile security breaches have been largely caused by unauthorized access to Personnel accounts resulting from passwords being stolen or guessed.
   2. It is vital therefore that every Personnel plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm QuickCover Insurance.
   3. In order to maximize the security of our information every Personnel 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 Personnel 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 Information Technology Officer of any changes to their role and access requirements.
* Report any security incidents or breaches, including suspected unauthorized access, to the Information Technology Officer promptly.
  1. Failure to comply with these requirements may result in the organization taking disciplinary action against the individual(s) concerned.

1. **System and Application Access Control**

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

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

* Creation of individual Personnel accounts
* Definition of roles or groups to which Personnel 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 (Personnel accounts and groups)
* Provision of varying views of menu options and data according to the Personnel account and its permission levels
* Personnel account administration, including ability to disable and delete accounts
* Personnel 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 Personnel has successfully logged on
  + Date and time-based logon restrictions
  + Device and location logon restrictions
* Personnel inactivity timeout
* Password management, including
  + Ability for Personnel 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

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

5.4. 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.

**References- ISO 27001:2013**

* A.9 – Access Control
* A.9.1 Business requirements of access control
* A.9.2 User access management
* A.9.3 User responsibilities
* A.9.4 System and application access control

**Acceptance of Terms and Conditions:**

Personnels must acknowledge and accept the terms and conditions of the Access Control policy and any associated agreements. This ensures their understanding and commitment to adhere to the policy guidelines and security requirements.

By implementing this policy, the QuickCover Insurance aims to maintain a secure and productive work environment. The policy ensures compliance with security best practices and applicable privacy legislation.

Declaration

I have read the Access Control Policy above and agree to comply with its contents and those of any other relevant policies of which QuickCover Insurance may make me aware.

Name of Personnel:

Signature of Personnel:

Date:

A copy of this statement must be retained by the personnel and QuickCover Insurance.