NCAG
Network Claim Assessors Group

Access control policy

1. Purpose

1.1. The purpose of the IT Access Control Policy is to ensure that all access to information assets is properly authorised, and that permissions to access information assets are maintained and reviewed.

2. Policy Objectives

2.1. To define the requirements of Network Claim Assessors Group, to ensure that access to information assets is subject to identification and authentication controls so that the authorisations granted as per this agreement are applied.

2.2. To establish the requirements for controlling access to Network Claim Assessors Group information or information that it is responsible for, including digital information and physical resources.

3. Policy Scope

3.1. This IT Access Control Policy shall apply to all access to all Network Claim Assessors Group information assets.

3.2. All Users provided with access to Network Claim Assessors Group information systems shall comply with this IT Access Control Policy as indicated in the Acceptable Use Policy.

3.3. Access to physical and non-physical assets will be governed under the same principles.

3.4. This IT Access Control Policy shall establish the logical and physical access control requirements for protecting the entire company`s information systems and hardcopy data.

3.5. This IT Access Control Policy shall cover access to IT facilities and data. Physical access of people to company sites is covered within the Physical Security Policy on site access control.

4. Policy Statement

4.1. This IT Access Control Policy forms part of Network Claim Assessors Group information Security Management System (ISMS) Framework as defined in the Information Security Policy.

4.2. This policy should be read in conjunction with Network Claim Assessors Group IT Acceptable Use Policy, which summarises what Network Claim Assessors Group deems to be acceptable use of information systems.

4.3. It is the responsibility of every User with access to the Company's information systems to ensure that they have read and understood this document. All Users are obliged to adhere to this policy. Any deliberate or informed breach of this Policy may lead to disciplinary action up to and including dismissal from the Company in accordance with the Acceptable Use Policy.

4.4. The IT Access Control Policy shall also apply to all Users who have access to the Company's information assets, including remote access.

4.5. Network Claim Assessors Group information systems are provided for business purposes only and this IT Access Control Policy is used to ensure that Users:

4.6. Comply fully with current legislation to Comply with other relevant Network Claim Assessors Group policies.

4.7. All Users, who use the Company's information assets and information systems, shall be responsible for safeguarding those resources and the information the Company may hold, from disruption or destruction.

4.8. The use of the Company's information assets and information systems indicates acceptance of this Access Control Policy.

5. Implementation Responsibilities

5.1. Network Claim Assessors Group IT team shall ensure that Users are provided adequate information of appropriate clarity to ensure compliance with this Access Control Policy.

5.2. Network Claim Assessors Group IT team shall develop, maintain and publish standards, processes, procedures and guidelines to achieve compliance with this Access Control Policy.

5.3. Annually review the Access Control processes, standards and procedures, to achieve compliance with this Access Control Policy and support the Access Control Strategy and provide security specific input and guidance where required.

5.4. IT asset owners (the individuals and teams who manage IT networks, servers and storage) and authorised users shall be assigned for each identified IT asset in order to approve or reject requests for access to their system.

Thys Botes

MD (Network Claims Assessors)

5.5. IT asset owners and authorised users shall check the validity of all user access requests to information assets owned by them before implementation.

5.6. IT asset owners and authorised users shall authorise employees requiring access to information assets owned by them.

5.7. Human Resources (HR) shall inform the IT department of users starting in, moving within and leaving the Company.

5.8. All appropriate managers shall authorise any requirement to changes to user's access rights on the information systems.

5.9. Users shall not share access codes and/or passwords, if access to other information systems are required, then a formal request shall be put forward for authorisation by an appropriate manager.

5.10. Users shall not share their physical access cards; if physical access to restricted areas is required, then a formal request shall be put forward for authorisation by the appropriate manager.

5.11. Users shall be responsible for the security (and secrecy) of their own secret authentication information. In no circumstances is secret authentication information to be shared.

5.12. Users shall ensure incidents are reported and escalated in-line with the Company's Information Security Incident Management Procedure.

5.13. The Company shall be responsible for ensuring all Users of Network Claim Assessors Group information systems read and acknowledge the policy principles extracted from this Access Control Policy and included in the Acceptable Use Policy.

6. Policy Principles

6.1. All information assets shall be "owned" by a named Network individual within Claim Assessors Group.

6.2. A process for user access requests, which mandates the steps to be taken when creating or modifying user access shall be defined, documented, annually reviewed and updated. The scope of this process must include network, application and database access and apply to any third-party access.

6.3. Access to information assets shall be restricted to authorised employees or contractors and shall be protected by appropriate physical and logical authentication and authorisation controls.

Thys Botes

MD (Network Claims Assessors)

6.4. Users shall be authenticated to information systems using accounts and passwords.

6.5. Users who have satisfied all necessary criteria may be granted access to information assets only on the basis that they have a specific need to know, or to "have-access to", those information assets.

6.6. Access privileges shall be authorised by the appropriate information Owner and allocated to employee, based on the minimum privileges required to fulfil their job function.

6.7. Administrator accounts shall only be granted to those users who require such access to perform their job function. Administrator accounts shall be strictly controlled and their use shall be logged, monitored and regularly reviewed.

6.8. Users with administrator access shall only access sensitive data if required in the performance of a specific task.

6.9. Users with administrator access shall also have an unprivileged account, which shall be used for all purposes not requiring administrator access, including but not limited to electronic mail.

6.10. Line managers, information asset owners and authorised users shall ensure rights and privileges granted to Users of information assets are reviewed at least every year to ensure that they remain appropriate and to compare user functions with recorded accountability. This shall include access to user accounts, which shall be revoked when they have been inactive for more than 90 days.

6.11. Access shall be granted only to those systems or roles that are necessary for the job function of the user. Regular maintenance will address the management of privilege creep.

6.12. Detailed processes shall be developed and followed for terminating, modifying, or revoking an employee's access.

6.13. In certain instances, particular access may be required for emergency reasons, such as undertaking emergency system maintenance. Requests for emergency access shall be directed to the Network Claim Assessors Group Head of IT, or a member of the Network Claim Assessors Group Management team and shall be approved by the information asset owner or authorised user. Requests and approval should be documented, if possible, before the change is required stipulating an expiry period,

which shall be enforced, for the access rights. A request for change shall be documented retrospectively where it is not possible to do this in advance.

6.14. All third-party access (Contractors, Business Partners, Consultants, Vendors) shall be authorised by an appropriate information Owner and, if necessary, monitored.

6.15. Third Party Access to information assets shall be granted in increments according to business need and identified risks. Information asset owners shall specify access timeframes and be prepared to offer justification for such access.

6.16. Remote access to Network Claim Assessors Group networks shall be appropriately authorised on a least privilege basis, with access only granted to systems and resources where there is an explicit business requirement. Only employees of the company or authorised third parties shall be able to connect to the company corporate infrastructure remotely.

6.17. Only authorised personnel shall be given access to secure areas at the company premises and any third-party premises where sensitive information is processed or maintained, or physical assets are held.

6.18. All access to areas hosting systems that store, process, or transmit sensitive data (e.g., server rooms) shall be controlled, monitored by cameras and logged. Logs shall be regularly audited, correlated with other logs and securely stored for at least three months, unless otherwise restricted by law.

6.19. In line with the site access policy all visitors shall have authorisation prior to entering any of the company facilities where sensitive data is processed or maintained.

6.20. All visits shall be logged, and details of logs retained for a minimum of one month, unless otherwise restricted by law.

6.21. Employees shall challenge and/or report any visitors found unsupervised or acting suspiciously at any site where sensitive Network Claim Assessors Group data is processed or maintained.

6.22. User account names and actions performed shall be recorded using Audit logging capabilities.

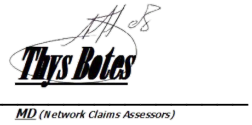
6.23. The Network Claim Assessors Group IT Team shall maintain plans indicating time schedules of all information security access audits to be performed across Network Claim Assessors Group to ensure compliance with this Access Control Policy.

Thys Botes

MD (Network Claims Assessors)

NCAG

Network Claim Assessors Group

Employee name THYS BOTES Employee signature 

Signed at PAROW on this 12 day of APRIL 2022