HUNTSWOOD

ACCESS CONTROL POLICY (ASSOCIATE VERSION)

APPROVAL CONTROL

TITLE	NAME	DATE
Risk Director	Helen Maslin	26/04/2021

VERSION CONTROL

VERSION	AUTHOR NAME	VERSION CHANGES	DATE
1.0	Jayne Morris	Associate version	31/10/2016
2.0	Jayne Morris	Updated to include requirement to remove pass when outside of the building	25/04/2017
3.0	Ethan Moore	Updated in line with Full Access Control Policy	26/04/2018
3.01	Jayne Morris	Update to access pass management	25/07/2018
3.02	Carol Hawker	Annual Review	08/04/2019
3.03	Carol Hawker	Annual Review	24/03/2020
3.04	Carol Hawker	Amendment to structure titles	24/03/2020
3.05	Carol Hawker	Review and sign off by Risk Director	26/04/2021
3.06	Craig Wooster	Annual Review Change of owner title Minor Amends	13/01/2022

TABLE OF CONTENTS

OBJECTIVE

The objective of Huntswood's Access Control Policy is to ensure access to information is controlled.

Access to information, computing facilities and business processes shall be controlled based on business and security requirements.

APPLICABILITY

Huntswood's Access Control Policy is applicable to all Huntswood's Representatives.

POLICY PRINCIPLES

1. Authorised User

1.1. Huntswood's Representatives will be considered as authorised users (allowed unsupervised access) to:

1.1.1. Physical resources (access doors, project rooms and secure doors); when the representative has been issued with a photo ID access card with access approved to the physical resource.

1.1.2. Computing facilities (computer network); when the representative has been issued with a unique USERID by Technology.

1.2. Access to physical resources or computing facilities shall be removed as soon as there is no longer a valid business reason for the access.

1.3. A Huntswood representative ceases to be an authorised user at the end of their contract period.

2. Access/ID Cards

2.1. Physical security is controlled by photo ID access cards. Photo ID access cards are issued by the Front of House Team, who will log the card and its owner in the access card register.

2.2. Photo ID access cards shall only be issued to a representative after receiving an approved new user request from HR or the appropriate line manager for the business area of the representative

2.3. All Huntswood representatives in Huntswood locations shall be issued with a photo ID access card.

2.4. Temporary and Contract staff working for short periods shall be issued with an access card (with photo) at the discretion of the manager of the relevant business unit.

2.5. Access rights for photo ID access cards shall be set up by the Front of House Team based on predetermined role profiles

2.6. All requests to make changes to access rights for role profiles must be made to the Technology service desk and will require approval by the manager of the business area in question.

2.7. Where access to Huntswood's head office space is required for a visitor (i.e. allocation of a visitor photo ID access card) approval will be required from the manager of the business area hosting the visitor. Approval must include confirmation of the start and end dates for the visitor's access.

2.8. Where access rights to Huntswood's head office space are requested to be added to the profile of any other individual other than a member of staff (i.e. an associate) approval is required from a director.

2.9. Photo ID access cards shall only be issued to individuals, no group or shared cards will be issued.

2.10. Photo ID access cards shall contain the following information:

INFORMATION	LOCATION	DESCRIPTION
Current employee photo	Front	The card will contain a passport style photograph, which is a good, current likeness of the representative.
Huntswood	Front	Current Huntswood's or subsidiary company logo.
Full Name	Front	The representative's full name.

2.11. The allocation of photo ID access cards shall be logged on badge control system. The card number may be used to identify and monitor the usage by Huntswood's Representatives.

2.12. Huntswood's Representatives shall wear their photo ID access cards when in Huntswood's offices. The Photo ID access card must always be displayed in a prominent position on the person. Photo ID access cards are not to be worn outside Huntswood offices and must be removed when exiting the building, even for short periods.

2.13. Photo ID access cards remain the property of Huntswood and shall be returned to the Front of House Team and securely destroyed (shredded) at the end of the representative's contract period or when the card expires.

2.14. Whilst failure to bring a Photo ID pass to work is not deemed to be acceptable, it is acknowledged that on occasion, and by exception, a member of staff may forget their photo ID access card. On such occasions they will immediately report to Huntswood reception to be issued with a "visitor" access card which the individual shall be required to return at the end of the day. Visitor passes shall provide access to the main office area for head office staff or the appropriate project area for associates only and shall be programmed to only operate for the day that it is issued.

2.15. If an access card is misplaced, lost or stolen Reception must be informed immediately and will cancel the card and reduce the risk of a physical or information security event from happening.

2.16. Monitoring and monthly reporting by the Front of House Team to the Director of Workplace Services shall provide detail of visitor cards issued to monitor individuals who repeatedly fail to bring their card to work.

2.17. All doors fitted with access card readers must remain closed (i.e. can only be accessed with an appropriate photo ID access card) with the exception of:

- Director's Offices - which shall be closed when not occupied
- Glass doors to Directors Office's and Board Room from reception shall be closed when the reception is to be unmanned for any significant period of time (i.e. more than 5 mins)
- Main reception doors are to be shut when only one member of reception team is present.

3. USERID

3.1. USERID's are issued and controlled by technology. USERID's shall only be issued through the "starters, movers and leavers" process.

3.2. USERID's shall only be issued to individuals; no group or shared USERID's will be issued.

3.3. USERID's shall be issued in the format <FIRSTNAME INITIAL><SURNAME>, for example; John Smith will be issued with a USERID of jsmith. In the case where there are 2 or more people that would create the same USERID i.e. John Smith and Jane Smith, it is acceptable to use a second initial or letter to uniquely identify the individual.

3.4. USERID's for Associates shall be issued in the format <uxxxx> ITRIS generated sequential number

3.5. Huntswood representatives shall not allow anyone else to use their USERID.

3.6. Where possible, USERID's shall match the USERID issued to the representative for all Huntswood's computing facilities.

3.7. All USERID's shall be issued with a temporary corresponding password that follows Huntswood's password policy in the Acceptable Usage Policy.

3.8. The usage of Huntswood's computing facilities shall be logged and the USERID shall be used to identify and monitor the usage of Huntswood's Representatives.

3.9. If a USERID is dormant, which is considered as not being used for 30 days, it shall be, reviewed with the relevant line manager and Technology and, if appropriate, then disabled by Technology.

3.10. If it is not known when the USERID will be used again, it shall be disabled by Technology; for example, accounts used by third parties for support or audit purposes.

4. Physical Access Control

4.1. Access to physical assets shall be approved by the asset owner.

4.2. It is the responsibility of the representative's line manager to request access to physical office space on a need-to-know basis.

4.3. Front of House Team are responsible for ensuring that physical access is granted to or removed from photo ID access cards after receiving an approved (by asset owner) access request from the representative's line manager.

5. Visitors

5.1. Visitors shall remain in the reception waiting area until being collected by their visitor host. Visitors shall not be allowed access to any other part of Huntswood's premises until they have been collected by their visitor host.

5.2. Visitors requiring access (e.g. Shred It, or someone working on site all day and does not need to be escorted) shall be provided with a photo ID access card on pre-approval of the relevant manager.

5.3. All visitors shall be signed in at reception and issued with a visitor badge – either paper pass for those being escorted or photo ID access card in line with the above. A record of all visitors shall be recorded in the visitor book. It is the responsibility of the visitor host to ensure their visitors have been signed in and issued with a visitor's badge.

5.4. Visitor hosts shall ensure that all visitors wear their visitor badges in a prominent position i.e. around their neck or on their belts and take responsibility for their visitor at all times.

5.5. All visitors issued with a paper pass shall be escorted by the visitor host or an appointed chaperone when on Huntswood's premises.

5.6. Visitor hosts shall ensure that all visitors return their pass at the end of their visit and that the visitor's time of leaving is logged in the paper passbook or logged electronically by reception where a photo ID pass has been issued.

6. Physical security

- The Chief Risk Officer, Chief Technology Officer, Director of Workplace Services, Facilities Manager and Head of Dev Ops and Sec Ops, are able to authorise out of hours work that requires building access and are the key points of contact for Premier Security. In addition, the IRT are authorised to make contact with Premier Security during an incident.
- During working hours, Facilities Manager is the first point of contact for any access issues or if the intruder alarm sounds.

7. File & Folder access

7.1. File & folder access shall be controlled using Access Control Lists (ACL).

7.2. To simplify the audit process of "who has access to what", File & Folder access shall be granted to groups (Active Directory groups) rather than individual USERID's.

7.3. File & folder access shall be granted to authorised users, on a need-to-know basis only.

7.4. Consideration shall be given to the classification of the information stored in the file or folder. To prevent information leakage, access shall not be granted to files and folders if doing so would allow a breach of Huntswood's Classification and Labelling Policy, which can be found on the group document repository.

7.5. Group membership shall be approved by the group owner, which is detailed in the group's description.

7.6. It is the responsibility of the representative's line manager to request access to files and folders via Huntswood's IT Service Desk where a ticket will be logged on the system and Technology will ask the business asset owner of the files and folder to approve the access request.

7.7. Technology are responsible for ensuring that group membership is granted to or removed from USERID's after receiving an approved access request from the representative's line manager or group owner.

8. Software Applications

8.1. Access to software applications shall be strictly controlled. The Chief Technology Officer is responsible for ensuring only legal software applications are used on Huntswood's computing facilities.

8.2. Only software applications approved by the Chief Technology Officer and sanctioned by the Chief Risk Officer shall be installed on Huntswood's computing facilities.

8.3. Software applications shall only be installed on computers for Huntswood's Representatives if there is a genuine business need for access to the software application.

8.4. Once access to software applications has been granted, USERID's shall be strictly controlled to ensure that USERID's are assigned the lowest level of access or least privileges required to carry out their duties.

8.5. It shall be discouraged from granting carte blanche or full access to software applications.

8.6. It is the responsibility of the asset owner to define appropriate access to the software applications that they own.

8.7. It is the responsibility of the representative's line manager to request access to software applications using Huntswood's Technology request system.

8.8. Technology is responsible for installing/removing software applications from Huntswood's computing facilities after receiving an access request from the representative's line manager that is approved by the system owner.

9. Remote Access

9.1. Security policy will be complied with to ensure data security.

9.2. Remote access to Huntswood's network shall be through a Huntswood approved access method.

9.3. Remote access via web enabled applications shall be encrypted using a Huntswood approved encryption standard.

9.4. Huntswood shall in exceptional circumstances, review and/or revoke remote access for example where an individual is:

- Under notice;
- Under disciplinary investigation.

10. Remote Control

10.1. The Huntswood Technology team use approved remote access tools or software to support the various IT Systems, as approved by the Chief Technology Officer.

10.2. Permission shall be sought from the user before "taking control" of their device. Ensuring any sensitive information is protected prior to remote access being granted. Refer to Huntswood's Classification and Labelling Policy.

11. Privileged access

11.1. Privileged Access is restricted and allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated in an e-mail from the user concerned, to their line manager who raises a request with the IT Service Desk setting out the reasons why the privilege is required and the length of time for which it is required. Technology will request approval from the Head of Risk before enabling any privileged Access.

12. Printers

12.1. Photo ID access cards provide access to the printers, which operate a coded release to the pass owner. An individual's printing cannot be accessed without the pass.

13. Audit

13.1. As part of Huntswood's commitment to ISO27001:2013 (Information Security), annual audits will be undertaken by the Internal Audit function. These audits will include reviews of all controls within this policy and reports on findings and recommendations will be issued to The Board and Risk & Audit Committee as appropriate.

TABLE OF DEFINITIONS

The table of definitions provides definitions of terms used within the policy document

TERM	DEFINITION
Huntswood Representative	Anyone who works for or on behalf of Huntswood.
Remote access	Remote access shall be considered accessing Huntswood's computing facilities from outside of a Huntswood office i.e. across the Internet

POLICY RESPONSIBILITIES

The following table defines the business roles and their responsibilities in regard of the policy document.

RESPONSIBILITY	ROLE	DEFINITION
Owner	Chief Risk Officer	The Owner ensures the policy is reviewed and maintained on a regular basis
Reviewer	Chief Risk Officer	The Reviewer ensures the policy document aligns with relevant legislation and company requirements
Author	Information Security Manager	Shall update the policy document in a succinct time frame on receiving updates from the reviewer and in accordance with company policy writing guidelines
Policy Audience	Huntswood Representative	Must apply the business policy to the business they undertake on behalf of Huntswood

APPLICABLE STANDARDS AND LEGISLATION

ISO/IEC 27001:2013

REFERENCE MATERIALS

The following are available on the group document repository:

Information Security Policy

Classification and Labelling Policy

Acceptable Usage Policy

Starters, Leavers and Movers Process