C2A POLICIES AND PROCEDURES
Access Control Policy

Table of Contents		
Section		Page

1. Introduction

1.1 Definition of Workplace

C2a is an alternative Internet and Phone Service Provider that provide competitively priced Fixed Wireless Broadband, ADSL Broadband, NBN and VoIP phone services at competitive and affordable prices while remaining local to Port Macquarie and surrounding areas.

1.2 Constitute – Access Control

C2a Access Control Policy is to eliminate risks of Unauthorized access to ensure the protection of c2a's facilities/information and equipment as well as the equipment of Shared Hosting Users within the Shared Server Room at C2A ECDC. This provides protection through controlled access which ensures respect of facility and through Employees and Shared hosting Users understanding their responsibilities for the use of the Shared Server Room. If this Policy is not followed access will be denied to Users.

1.3 Filing and Storage of documents

This policy and Procedure are displayed in the office of the business and must be accessible to all staff, contracted persons and Shared Hosting Users.

Complaints and incident reports- must be filed and kept for a minimum of 7 years.

2. Purpose of this Document

Is to ensure the protection of resources and information stored by c2a or by a Third Party On their own infrastructure against accidental or malicious damages, modification or destruction. The resources and Information stored by c2a for shared hosting users is an important, valuable asset which must be managed with care. All information is valuable to all shared hosting & Co-Location Users and must be treated as such.

Access controls are put in place to protect Shared Server room access and information by controlling who has the rights to use the shared server room and resources c2a provides by shared hosting and by guarding against unauthorised use.

Formal procedures are in place to allow access to the server room and information of enrolment entry and exit are recorded by RF tag entry as well as IP camera 24/7.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3. Persons affected

- Employers
- Workers (Employees, Contactors) in office areas (on-site areas)
- Shared Hosting Users

4. Definitions

- PCBU: Person Conducting a Business or undertaking
- Shared Hosting Users: Customers who use our premises for hire for hosting purposes
- Office areas/On-site: These include the Office, Server Room and Storage Shed
- Off-site areas: Houses/Business' where workers perform installs of our services
- Access control: Access control rules and procedures are required to regulate who can access the Server Room in the office. This policy applies at all times and should be adhered to whenever accessing the server room.

5. Responsibilities

5.1 (PCBU) Director/Officer/Manager/team leader

- To ensure Policies and procedures are accessible and followed
- To provide an orientation to shared users, sign forms required to use these premises and read Policies
- To ensure access to the data centre is only for users with permission
- To ensure all shared users respect other users property
- To change passwords when needed
- To control FOB access e.g. to replace Fobs when needed or cancel access when needed

5.2 Shared hosting users

- To sign in on arrival and sign out on departure
- On departure ensure all doors are closed and locked – door to shared server room and front door
- To be respectful to c2a property and equipment
- To be respectful of other Shared Server Room Users
- To keep your own equipment neat and tidy
- To follow policies, rules and procedures in place (have access to policies in policy book)
- To be aware of procedures in case of, for example, fire evacuations, accidents

- Any damage to c2a premises/equipment or other Shared users equipment must be replaced and/or will be charged at the appropriate rate.
- Use your own tools and equipment – safety is your responsibility
- Ensure work is carried out in a safe manner
- No food or drinks in the Shared Server Room
- No alcohol or drugs on the premises
- Let c2a know if FOB is lost - c2a can deny access to lost FOB and provide a new FOB
- You may not share your FOB with another person
- You may not Permit anyone to access secure areas with your FOB (this contravenes c2as rules regarding secured access and access may be revoked).
- You may not allow unregistered persons into the Server Room with fingerprint access

6. Risks

This policy is intended to eliminate the risks of unauthorized access to the Office and Shared Hosting Server Room. c2a provides access to shared hosting infrastructure via FOB, to the office, as well as finger prints access to the Shared Server Room used for hosting purposes. This protects the information and resources stored by c2a and third party co-located users.

To further protect the facility, c2a has security cameras set up to ensure all workers and users use the facility respectfully i.e. c2a's property and the property of other shared hosting users.

7. Applying the policy – Access

7.1 Management Access

Passwords

Only Management knows passwords to the building, this is to ensure safety if there are any problems passwords can be changed. This ensures safety from general public, as well as, Users giving passwords out.

7.1.1 Weak and *strong* passwords

Management decides passwords to the main entrance. This password can be changed accordingly. Only Management have passwords.

Each shared hosting user is provided with a FOB to allow easy access and eliminate forgetting password and leaking password problems.

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Management uses strong passwords with a minimum standard of:

- At least seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

7.1.2 Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times.

- Never reveal the password.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different c2a systems.
- Do not use the same password for systems inside and outside of work

7.2 Access for Shared Hosting clients

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. These must be agreed by the c2a director. Each user must be allocated access rights and permissions to systems and data.

Shared Hosting Users on acceptance are to sign that they agree to terms and conditions of the use of the room, as well as read and sign related Policies needed for their safety and the safety of others.

Shared Hosting Users need to follow the following steps to use the Shared Server Room:

1. Sign in registration with time on arrival
2. Are commensurate with the tasks they are expected to perform.
3. Have unique access that is not shared with or disclosed to any other user or person i.e. the FOB
4. Have an associated fingerprint password that is requested on access to shared server room.
5. To leave room the same as when first came (keep things in a neat and orderly manner)
6. To sign out with time when leaving

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated.

C2a provides FOB keychain to enrolled users to ensure security for access into the building. FOBs are the first line of defence for our ICT systems.

For further access into the Shared Hosting Server Room Certain people are allowed to enter and will need finger print enrolment. The Technician will be inducted and enrolled accordingly.

If there is any problems with clients FOBs they can also be cancelled to further provide safety. This may include but not limited to:

- losing FOB
- not following policy and procedures
- damage to c2a property and premises as well as other hosting property within the Shared Hosting Server Room

Ensure that the FOB is protected and **advise straight away if it goes missing** so that it can be cancelled at any time.

Advice of lost or stolen FOB Keychain can be sent to us via e-mail to info@c2a.com.au

7.3 User Registration

A request for access to the data systems must first be submitted to the director of c2a for approval. Applications for access must only be submitted if approval has been granted by the Director. There is a form to read and sign to ensure users completely understand their responsibilities and obligations to use the premises. They must also read and sign relevant Policies and Procedures such as emergency

evacuation plan, incident/accident procedures and complaints and grievance procedures.

7.4 User Responsibilities

It is a user's responsibility to prevent their user ID – FOB from being used to gain unauthorised access to Office and Shared User Room:

- Following the Password Policy Statements outlined above in Section 7.2.
- Informing Director of any changes to their role and access requirements.
- Protecting FOB from further use from unauthorised persons.

Further responsibilities

Please see section 5, 5.2 for shared server room users responsibilities.

7.5 Network Access Control

The normal operation of the network must not be interfered with as it can compromise the security of the network. Specific approval must be obtained from the Director before connecting any equipment to c2a's network.

Users using the Shared Hosting Server Room are only to touch their own equipment, unless authorised by c2a Director after being given consent by initial party/shared hosting user. If one shared hosting user touches another shared hosting users equipment and has permission from the initial party, access or historical documents must show this or c2a must be informed of such undertaking. C2A is not responsible if any failures occur as a result.

8. Policy Compliance

If any user is found to have breached this policy, they may be subject to c2a's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the director.

9. Policy Governance

The following table identifies who within c2a is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.

- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Director of Company
Accountable	Director of Company
Consulted	Director, Administration, employees
Informed	All Employees, All Temporary Staff, All Contractors, Shared Hosting Users

10. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Appendix

C2A/ECDC Access Form

User Information

Full Name: ..... Date of birth: .....

Address .....

Business Name: .....

Business Address: .....

Email: ..... Phone Number: .....

Next of Kin name (in case of emergency): .....

Next of kin contact number: .....

Action (choose/tick one or both):
FOB Access (c2a Front door) ☐
Finger Print Enrolment (ECDC Shared server Room) ☐

Reason for access to c2a premises/Shared Hosting Server Room:

Access to c2a premises and/or Shared Server Room:
You will be given a FOB to access the c2a premises and/or finger print access to enter the Shared Server Room. These are only to be used by authorised persons. Please ensure you take care of the FOB and let c2a know if FOB is lost. C2a can then deny access to lost FOB and provide a new FOB.

There is also 24 hour surveillance camera to further ensure security of access.

Responsibilities:

- To sign in on arrival and sign out on departure
- On departure ensure all doors are closed, locked and secured – door to shared server room and/or front door
- Ensure the premises are left in the same order as when you arrived
- To be respectful to c2a premises, property and equipment
- To be respectful of other Shared Server Room Users equipment
- To take care of other property within the room and only touch their own equipment
- To keep your own equipment neat and tidy
- To follow appropriate policies, rules and procedures (users have access to policies in policy book)
- To read and sign any policies required

- To know procedures in case of, for example, fire evacuations, accidents
- Any damage to c2a premises/equipment or other Shared users equipment must be replaced and/or will be charged at the appropriate rate
- Use your own tools and equipment – safety is your responsibility
- Ensure work is carried out in a safe manner
- Let c2a know if FOB is lost - c2a can deny access to lost FOB and provide a new FOB
- To clean up any messes for example, in Shared Server Room or Kitchen

You May Not:

- Share your FOB with another person
- Permit unauthorised access to secure areas with your FOB or finger print
- Have food or drinks in the Shared Server Room
- Have alcohol or drug use on the premises
- Enter c2a Admin Office or Directors Office unless granted further permission from director

If these responsibilities are not followed or irresponsible behaviour occurs, then c2a/ECDC can deny access to areas. When taking equipment from the premises, a supervisor may be present.

By signing below you acknowledge that you will abide by the policies, rules and procedures that govern access to c2a premises and/or ECDC Shared Server Room.

User Signature: ..... Date: .....

Supervisor Signature: ..... Date:.....