Information Technology Policy & Procedures

CBSA

COMPLETE BUSINESS SOLUTIONS AUSTRALIA

Purpose

The computers, information and technology provided by Complete Business Solutions Australia (CBSA) are considered corporate resources and are to be used in accordance with the guidelines as set out within this policy and procedures. This policy ensures that emails, internet usage and other electronic communication is properly used at all times and that CBSA is protected from actions of fraud, error, defamation, discrimination, harassment and privacy violation.

Policy

1. Computer logon

1.1. CBSA provides all staff members with a user name and password to access the computer system and services provided at CBSA.
1.2. All staff must ensure they keep their login details secure and protected.
1.3. This login will provide access to email, internet and the organisation's cloud-based file storage and services
1.4. All files must be accessed and saved according to Document Management Policy & Procedures.

2. Acceptable use of systems

2.1. All electronic, information and technological resources provided by CBSA are for business use only. They are only to be used for the purpose of performing authorised lawful business activities. The downloading, viewing, distribution and/or copying of non-business material including but in no way limited to pornographic, offensive or discriminative material is not permitted.
2.2. Should staff make incidental use of the email system to transmit personal messages, such messages shall be treated no differently from other messages and, as such, CBSA reserves the right to access, copy or delete all such messages for any purpose and to disclose them to any party deemed appropriate by the system owner.
2.3. Personal use of email facilities shall not:

- Interfere with normal business activities.
- Involve any form of solicitation.
- Be associated with any for profit outside of business activity.
- Potentially embarrass or offend CBSA or any staff member, or client of CBSA.
- Break privacy, copyright or intellectual property laws.

3. Non-acceptable use of systems

3.1. CBSA will not tolerate the use of any of its electronic, information and technological resources for the sending, receiving or forwarding on of emails or communication which is:

- Defamatory in content.
- Discriminatory, racist or sexist.

- Abusive, obscene or where language content could be considered offensive.
- Sexually harassing.
- Pornographic.
- Junk-mail, such as chain letters and non-business graphics, audio and sound.
- Internal appeal.

3.2 The opening of email attachments from untrusted or unknown sources is not permitted.

4. Emails

4.1. Emails sent externally or internally are sent by an individual representing the company and should be treated in the same way as written correspondence. All outgoing emails must include salutations and a staff member's CBSA signature including disclaimer.

5. Monitoring

5.1. All messages and associated file attachments sent by employees of CBSA are the property of CBSA.

5.2. CBSA has the right to read, monitor, track, record, copy or delete the contents of a staff member's mailbox at its discretion.

5.3. CBSA has the right to monitor, track, or record an individual's use of the Internet.

6. Liability

6.1. Comments that are not appropriate in the workplace are not appropriate on the email network.

6.2. CBSA understands that it may be liable for what its staff write in email messages. The audience of an email message may be unexpected and widespread. Staff must not assume that email messages are private or secret. Email messages can be easily copied, forwarded, saved, intercepted, archived and could be the subject of discovery if CBSA is involved in litigation.

6.3 All information stored in email accounts is considered to be 'documented' and therefore are discoverable in litigation. It is therefore the responsibility of every employee to refrain from using unnecessary or inappropriate messages on email.

7. Confidential information

7.1. The transmission of commercially confidential information to competitors, affiliates, other organisations and external entities or persons of CBSA and its clients is not permitted.

8. Storage of information

8.1. All staff are required to store files as they are created and/or adjusted on the cloud-based file storage system in the folder relevant to the quality area it relates to.

8.2. All electronic folders include an ‘Archived’ folder where non-current versions are to be stored as a new one becomes available.
8.3. Staff are expected to ensure that the cloud-based storage system is kept up-to-date and accurate at all times and ensure the correct use of the **Document Management Policy & Procedures** policy at all times.

9. Compliance with policy

9.1. If any person at CBSA becomes aware of the misuse of email or the internet, that person should immediately report it to Senior Management for investigation.
9.2. If any person is offended, humiliated, intimidated or embarrassed by the use of an email or Internet by other employees, that person should also report it to Senior Management.
9.3. CBSA is committed to the terms of this policy and will thoroughly investigate and deal with all incidents of breach of this policy.

Procedures

1. Accessing the computer system

1.1.Login instructions
1.1.1. Each staff member will be provided with a personal login and password for the computer system.
1.2. Keep passwords secure.
1.2.1. Passwords are to be kept secure and private at all times.
1.3. Deactivate passwords at the end of employment.
1.3.1. At the end of employment these passwords will be deactivated.

2. Accessing emails

2.1. Email address instructions
2.1.1. All staff will be issued with an email address upon induction.
2.1.2. The email account must be used in strict accordance with the **Information Technology Policy**.
2.1.3 Any emails should conform to the **Email Template** requirements.
2.2. Ensure email signature is included in outgoing emails.
2.2.1. All outgoing mail is to include the standard organisational email signature with the relevant details of the staff member included.
2.2.2. The signature will include the standard disclaimer.

3. Accessing software programs

3.1. Software administration

3.1.1. Access to software programs such as the email client will be set up and provided upon commencement of employment.

3.1.2. Passwords are to be kept secure and private at all times.

3.1.3. At the end of employment these passwords will be deactivated.

4. Accessing the cloud-based storage system

4.1. Software administration

4.1.1. All files are stored on the cloud-based storage system in a manner that enables staff to locate files in a logical manner.

4.1.2. Staff must always save working documents onto the cloud-based storage system rather than on their individual computers.

4.1.3. Files must be saved in a logical order so they can be easily retrieved and located by other staff.

4.1.4. Staff must ensure that no files are deleted from the server. Files must be moved into the "Archived" folder if they become obsolete due to a new version.

5. Resolving equipment faults

5.1. The person who identifies the fault is to contact IT Support staff member

5.2. The IT Support staff member is to raise a support ticket on the support software

5.3. The IT Support staff member is to then investigate and try and resolve the fault

5.4. If they resolve the fault then they close the support ticket, otherwise they escalate the support request to senior IT staff members

5.5. The senior IT staff members are to then investigate and try and resolve the fault

5.6. If they resolve the fault then they close the support ticket, otherwise they escalate the support request to the equipment/software manufacturer or vendor

5.7. If the equipment/software manufacturer or vendor can resolve the problem then the IT support ticket should be closed. If they cannot resolve the problem then the support ticket should be closed as unresolved.

Related policies, procedures, forms, and documents

The following are related to this policy and procedure:

- IM002 – Document Management Policy & Procedures
- TM001 – Email Template

Document Control

Document No. & Name:	**HR002 – Staff Management Policy & Procedures IM005 – Information Technology Policy & Procedures**
Quality Area:	HR – Human Resources IM – Internal Management
Author:	Complete Business Solutions Australia (CBSA)
Status:	Approved
Approved by:	Henry Thomas
Approval date:	26/10/20XX
Review date:	27/06/20XX
Standards:	No standards are linked to by this policy and procedures.