Security Guidelines for Working in Shared Premises and exchanging information

The business information of the Commonwealth Bank of Australia (**Bank**) is a valuable asset and the Bank is committed to keeping it secure. It is everyone's responsibility to ensure the confidentiality, integrity and availability of the information and assets of the Bank and its customers is preserved.

In addition to legal requirements, the community, our customers, shareholders and colleagues have an expectation that the Bank maintains a high level of security over its information.

This is particularly important during transition or knowledge transfer stage of project and there are a number of Bank and Bank Technology Partner / Service Provider staff involved in sharing or transitioning various forms of confidential information. During this period, it is imperative that Bank staff as well as the Technology Partner staff are aware and take adequate measures to protect the Bank's information and intellectual property. Please note that any reference to "Bank information" or "confidential information" includes information and intellectual property not owned by the Bank but which is under Bank control.

Bank Policy

Your duty to protect the privacy of customer information forms part of the Statement of Professional Practice. The Federal Government's National Privacy Principles reinforce the need to keep customer information totally confidential.

The Information Security Policy, Information Technology (IT) Security Policy provides guidance on all matters relating to Information and IT Security and it is everyone's responsibility to ensure that they are conversant with their responsibilities.

All of the Bank's Security procedures apply in shared facilities, transition stages and document handover stages however you need to pay particular attention to the following precautions to protect the Bank's computer system and information from inappropriate and unauthorised access.

Note: Inappropriate or unauthorised use of the Bank's computer systems will result in disciplinary action, which may result in dismissal.

Electronic Information

- Ensure that confidential information displayed on your computer screen can not be viewed by others
- Screen lock your workstation **<u>at all times</u>** when unattended (even when away from your desk for a short time)
- Log off all Bank systems prior to leaving work
- Ensure all electronic storage media such as floppy disks, CD-ROM's, USB memory sticks are securely locked away
- Ensure confidential information is not transmitted outside the CBA environment in electronic or hard copy form, without a valid business justification. If confidential information needs to be transmitted to external parties, then it must be encrypted in transit.
- Under no circumstances should application source code or CBA customer data be emailed or transmitted in electronic or hard copy form, without prior approval from EIT Security.
- Handover and or sharing of confidential information between CBA and Technology Partners must be in a controlled manner (with a document register setup to log all documents shared).

Hard Copy Information

- Collect printer output immediately.
- Clear fax machines regularly.
- When you are finished working on sensitive documentation, ensure it is securely locked away.
- Clear all sensitive documents and papers from your desk **<u>at all times</u>** when unattended. (even when away from your desk for a short time)
- Ensure all hard copy information is securely locked away prior to leaving work
- Shred all unwanted copies
- Handover and or sharing of confidential information between CBA and Technology Partners must be in a controlled manner (with a document register setup to log all documents shared).

Sharing of Information

- Do not write down or record your UserID and password - others may use this to access Bank and Customer data
- Do not share your UserID or password with anyone, not even your Manager
- Do not discuss information with a person unless they have a *Need to Know*
- Do not discuss sensitive information, Bank processes or system information where people can

overhear the conversation

Physical Security	• Access cards are to be used by the authorized holder only and are not to be shared under any circumstances. • Do not allow people to 'tailgate' (follow you) into a restricted area without swiping their own access card. • Do not wedge or prop doors to restricted areas open, and always make sure such doors are closed behind you. • Identify any strangers you see on your floor or in your building and validate their reason for being there. • Should it be necessary to remove a laptop, any type of magnetic or electronic media, or hardcopy containing Bank information from Bank premises, you are to ensure that it remains in your possession at all times and is not left unattended, particularly in public places such as restaurants, hotels, airports or train stations. • Do not leave your bags or other possessions unattended in Bank buildings where they might cause a security incident. • Do not leave valuable items unattended on your desk or in unlocked drawers, or cupboards. • Be alert to suspicious behaviour in or around Bank buildings and report any concerns to the Group Emergency Hotline on 1800 643 410 from within Australia or +61 2 9777 2444 from overseas
Fraud and Unethical Behaviour	• The Bank has zero tolerance towards fraud or corrupt behaviour. All matters where fraud or corruption is suspected will be reported to the relevant law enforcement agency. • Fraud and corrupt behaviour can be perpetrated either by personnel within the Bank (Internal fraud) or outside the Bank (External Fraud). • You must report all allegations, suspicion or detection of fraud or corrupt behaviour to Group Security: ○ Internal Fraud: From within Australia: 1800 738 856 From overseas: +61 2 9151 6420 ○ External Fraud: From within Australia: 1800 023 919 From Overseas: +61 2 9777 2444
IT Security Incidents	• Make sure that you change your password if you suspect that it has been compromised • If you suspect that an Information security incident has occurred please contact the CBA EIT Security hotline number (+61 414 730 371), or email address (infosec@cba.com.au) immediately.

Further Information

Hard-copes of relevant policies have already been provided. Electronic versions and further Information is available in CBR and Security Central:

- Statement of Professional Practice http://commnet.cba/cbr/PER/PER00047.htm
- Information Security Policy http://commnet.cba/cbr/POM/POM00001.htm
- Information Technology and Telecommunications (IT&T) Security Policy http://commnet.cba/cbr/IT2/IT200009.htm
- Workplace Requirements for Expected Computer Use http://commnet.cba/cbr/PER/PER0009E.htm
- Information Classification and Handling guidelines use http://commnet.cba/security_central/policy/docs/Information_Security_Classification_Standard.pdf
- For a complete set of policies use http://commnet.cba/security_central/policy/index.asp

Acceptance of Accountabilities

Team Member: (Must be a Technology Partner staff member who is working on CBA premises) I have read and understood my responsibilities and agree to comply with these guidelines regarding working in shared premises		
Name with SAP Number	Signed	CBA Joining Date