



## Secure Computing for Financial Transactions

We strongly recommend the following computer security settings and control procedures as part of your efforts to secure your sensitive data and transactions. These steps are important in your dealings with SunCorp and other financial service providers:

### **Restrict Administrative Rights**

User accounts should be created as general users with permissions to use services but not install any software. Operating system administrative rights and permissions should be restricted to administrators only.

### **Utilize Current Anti-virus (malware/spyware) Software**

Ensure anti-virus software is properly installed and configured, software version is current, updates are applied, virus-signature files are current, and that there is a tested process for frequent signature file updates (at least once a week). In addition, a full system scan should be completed once a week.

### **Utilize Personal Firewall Software**

Even if a network firewall exists, ensure that the personal firewall is properly installed and configured, and is regularly updated. Adjust the software settings as appropriate for the environment. Note: Ensure the installation of the personal firewall does not conflict with other security before implementation.

### **Operating System/Software Patch Management Process**

Ensure patch management procedures are in place and tested for third-party applications and Windows operating systems and applications.

### **Workstation IP Address Lockdown**

If products or services allow IP address lockdown as a user option, ensure that this control is used. For example, SunCorp's APEX ACH System has IP address lockdown features available for activation at the user level.