Model information security provision

User IDs and/or passwords will not be written down and kept within the general area of the computer. Users will not utilize internal passwords or substantially similar passwords on external systems (websites, web based email, etc.).

Users will not allow any person to access, in any manner, their assigned computer equipment unless that person is specifically authorized to do so. Users should not disclose their login IDs or passwords to anyone.

The loss of any computer equipment or any of [the Company]’s information must be immediately reported to [appropriate officer, such as the Director of Information Systems] who will immediately ensure that all possible steps are taken to protect [the Company] from further information loss.

Any attempt by another person to obtain a login ID and/or password, or any other suspicious activity, must be immediately reported to [appropriate officer, such as the Director of Information Systems].

Users shall take all reasonable measures to protect [the Company]’s systems from damage due to viruses, “Trojan horse” programs, and similar problems. Users should exercise extreme care when using the Internet or email and should open only those attachments that are work-related and from a known sender. If a message is intercepted and quarantined by [the Company]’s virus scanning software, the User should notify the sender that this has occurred and that their system is probably infected with a virus. If infected emails continue to arrive from that email address, then User should block all email from that address until the infection has been rectified.

All Users will ensure that their computer files are properly backed up. This means ensuring that:

• Their files are stored on servers that are part of a regular back-up routine; or

• Making their own backups, ensuring that they are removed to an off-site location, having clear documentation associated with their back-up procedures, and making the documentation accessible to departmental management.

[Appropriate officer, such as the Director of Information Systems] will ensure that all security updates for operating systems, web browsers, server based applications, and email clients are installed as soon as they become available.

[Appropriate officer, such as the Director of Information Systems] will ensure that the hard drive of any computer to be discarded or sent out for repair will have all sensitive and/or confidential information removed from it.