Policy #: IT.009–Virus Controls

Governed by: IT Administration
Approval Date: November 1, 2016 **Last Updated:** November 1, 2016
Purpose: CEO Password Controls

CEO Anti-Virus and Controls

Users should be wary of any odd alerts or virus alerts and they must report this immediately to the IT Department/Staff. Users should note that there have been some cases, although not always, in which such warnings/alerts have been hoaxes that nevertheless waste time and effort and cause unnecessary panic if passed on to others. Users must, therefore, only pass on such warnings to the IT Department and Staff.

Users that are working remotely on their own personal computer (PC) or laptop must ensure they have their own anti-virus system installed an up to date. Users must disclose information about their antivirus system to the IT Manager if requested. Any users that do not have a sufficient antivirus system deemed by the IT Manager will not be allowed access to the network from a personal device.