WESTFIELD INSURANCE®

A Guide to Protecting Your Digital Assets

- □ Regularly update the passwords to your servers, internal sites, email, etc. at least once per quarter. Similarly, passwords should not be obvious; they should be a mix of numbers, upper and lowercase letters, and symbols.
- □ Consider investing in a password management tool, like LastPass or Sticky Password to help keep track of each of your logins.
- □ Do not open unknown email attachments, or emails received from an unknown contact address.
- □ Install firewalls on yours and your employees' computers and adjust the settings for it to automatically update.
- □ Shred any confidential information, or lock it away for administrator use only if needed.
- □ Do not leave personal or confidential information on paper out in the open. Similarly, do not write passwords down on an open notebook or post-it.
- □ Restrict access to servers, folders and files to only the employees who need access as part of their job.
- □ Never leave your laptops, tablets, mobile devices or other technology unattended. Should your equipment be stolen or left unattended for a prolonged period of time, encourage employee to do a remote wipe of stored information and data.
- □ Implement a workplace policy that requires employees to report stolen equipment immediately so that proper security measures can be taken as soon as possible, which will minimize the threat of stolen information.
- □ Avoid using unsecure wireless internet connections when away from your office. These are often easy targets for hackers.
- □ Develop an encryption policy for all employees to follow on their laptops or other tech hardware.
- □ Require mobile devices, applications and operating systems to be regularly updated with new releases of software to ensure the latest security features are installed.
- □ Require a passcode for mobile devices in which employees are accessing company information on during the work day.
- □ Adjust the settings on all mobile devices and laptops to turn on GPS-tracking capabilities.