Laptops and Mobile Devices

The laptops and mobile devices provided by the Company remain at all times the property of the Company and must be returned to the Company upon resignation/dismissal or at any other time upon the Company's request. Employees are responsible for taking reasonable precautions to secure their devices and computing environment.

Any employee who is assigned a laptop or mobile device (on a full-time or loaner basis) must:

- Never leave the device visible in a parked vehicle (locked or otherwise);
- Never place the devices in checked luggage at the airport or for other forms of travel;
- Never let anyone else, including friends or family, use your equipment;
- Always have the devices with you in a taxi or car service and not in the trunk; and
- Only store Confidential Information (as defined in this Handbook) on the Company network or Company approved Cloud Network - never store Confidential Information on laptops, mobile devices, home computers, or USB "thumb drives."

Any employee who uses any device (Company issued or personal) to access Company data or systems must:

- Never save Company passwords on the hard drive of laptops or mobile devices;
- Configure the device to lock after a period of inactivity and require a PIN or password for access;
- Configure multi-factor authentication for mobile devices;
- Enable encryption on all devices;
- Always lock your screen when you're away from your device; and
- Notify the IT and Legal Departments immediately if your laptop or mobile device is lost or stolen.

Any employee who discovers misuse of the Computer Systems should immediately contact his/her/their supervisor or the IT Manager. Every Company employee is responsible for using the Computer Systems properly and in accordance with this policy. Any questions about this policy should be addressed to the Human Resources Department or the IT Manager. Violations of these policies may result in disciplinary action, up to and including discharge.