# IT Asset Management Policy

## Summary

IT asset management is vital for maintaining the lifecycle of the technology in use by the company in a way that optimizes value and efficiency for all employees. It is important to have a strategy in place for maintaining, upgrading, purchasing, and decommissioning IT assets as needed. Poor asset management can have negative effects on productivity and staff morale as assets necessary for their roles become difficult to locate. It is the company’s ongoing commitment to insure all employees have the necessary tools to work effectively in their role.

## Purpose

The purpose of the IT Asset Management Policy is to maintain accurate records of the IT assets owned by GeoSpectrum Technologies Inc. This policy establishes procedures to ensure the safeguarding of the company’s IT assets. IT asset tracking is a vital part of the process of safeguarding the company’s assets. The benefits of this include:

1. More efficient maintenance of equipment;
2. Present and future IT asset needs being more accurately assessed;
3. Insurance of the assets; and
4. Security of sensitive information.

## Scope

This policy applies to all users of all IT assets owned by the company.

IT assets include:

1. Desktop and laptop computers;
2. Laptop accessories;
3. Monitors;
4. Uninterruptible Power Supplies, (UPS);
5. Printers/Scanners;
6. Mobile data devices such as smartphones and tablets; and
7. Any other IT peripheral equipment.

## Policy

### IT Asset Tracking

All IT assets belonging to the company are recorded on an ongoing basis in an IT asset tracking register, maintained by the IT department, and tagged with an identification sticker. All employees will be required to sign an IT Asset Undertaking letter shown below:



To assist in keeping the register accurate, all employees are responsible to adhere to the following:

1. IT assets owned by the company shall not be removed from the company premises except under the following circumstances:
2. The IT asset is issued with the purpose of being used remotely for business purposes. These items include:
3. Laptop,
4. Cellular device, and
5. Accessories related to previously stated items.
6. If an exception has been made to this policy that has been requested and approved by the IT department and the Company Security Officer (CSO).
7. All assets not accounted for in the IT Asset Undertaking letter issued to and signed by the employee must be signed out with the IT Department. An expected return date must be provided. If this expected return date must be extended, employees must communicate this to the IT department. If not returned by the expected date and there is no communication with the IT department, the IT department reserves the right to recover the asset(s) immediately.
8. If any assets are to be moved, reassigned, or returned, the IT department must be consulted.
9. In the event of loss, theft, or damage, employees are required to report the loss to the IT department immediately it becomes known.

All assets purchased by the company are property of the company and are expected to be returned to the IT department in the same condition as issued upon cessation of employment.

All employees are required to read and sign the IT Asset Undertaking letter. Upon receiving this letter, the IT department will have already completed the information in respect of the asset(s). All employees should review the information prior to signing the undertaking.

### Procedures for Mobile Asset Safeguarding

All employees are responsible for safeguarding any IT assets they remove from the premises. This includes maintaining physical control of all assets, and in the event that is not possible, securing the asset(s) appropriately.

The employees in possession of a company laptop, cellular device, and accessories related to these assets, are responsible for the physical security of these items by taking the following precautions:

1. Do not leave the asset(s) in an accessible place outside of the company’s facility unattended.
2. Do not allow use by anyone other than the assigned user.
3. Do not use the asset(s) for personal use.
4. When not in use outside of the company’s facility, the asset(s) must be locked away securely and out of sight.
5. Do not leave the asset(s) anywhere with extreme temperatures.
6. Do not use the asset(s) in locations that might increase the likelihood of damage.
7. Do not make any physical modifications to the asset(s).