Incident Response and Handling Policy

Effective day **1 October, 2019**

This Incident Response and Handling Police is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the Sage Seller private network.

1. Users must report suspected virus attack instances, suspicious e-mails, popup windows, or unusual programs to the local systems support provider, who must in turn report the incidents to the incident response team or management assigned staff.
2. Users without a support provider must report suspected virus attack instances, suspicious e-mails, popup windows, or unusual programs to the incident response team or management assigned staff.
3. Users must report unusual messages or mailbox activity to the incident response team or management assigned staff.
4. If an account or password is suspected to have been compromised, immediately report the incident to the incident response team or management assigned staff and also immediately change all passwords.
5. Workers have an obligation to report suspected fraudulent activity to the incident response team or management assigned staff.
6. When business declares an electronic security incident, such as one involving a virus or other software threat, personnel must follow all procedures to identify, contain, and recover from damage that may result from such threat.
7. Workers experiencing loss of confidential information, laptop computers, smart mobile devices or other electronic storage devices must immediately report the loss to the incident response team or management assigned staff.
8. Business or location should comply with the incident response team or management assigned staff procedures. Compliance with this includes but is not limited to:
    - Business or Location should train its workers to identify, respond to and report Information Security Incidents.
    - All employees, contractors and third party users of information systems and services must report any observed or suspected security weaknesses in systems or services.
    - Workers should not attempt to interfere with, prevent, obstruct, or dissuade another worker in their efforts to report an Information Security Incident or retaliate against an individual reporting or investigating information security problems or violations.
    - Workers should not be subject to retaliation or other adverse consequences for reporting Information Security Incidents.
    - Business or Location should submit as appropriate, a Security Incident Report to the incident response team or management assigned staff team to be implemented in the Incident Report Tracking Database.

Responsible Person: Illia Cheherst