POLICY STATEMENT

Annex A reference
A.16 Information security incident management
A.16.1.5 Response to information security incidents
A.16.1.6 Learning from information security incidents

Peak Collections has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing Peak Collections employees, partner agencies, contractors and vendors of the importance of the identification, reporting and action required to address incidents, Peak Collections can continue to be pro-active in addressing these incidents as and when they occur.

All Peak Collections employees, partner agencies, contractors and vendors are required to report all incidents – including potential or suspected incidents, as soon as possible to Peak Collections's data manager.

The types of Incidents which this policy addresses include but is not limited to:

COMPUTERS LEFT UNLOCKED WHEN UNATTENDED:

- Users of Peak Collections computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All Peak Collections employees, partner agencies, contractors and vendors need to ensure they lock their computers appropriately - this must be done despite the fact that Peak Collections computers are configured to automatically lock after 5 minutes of idle time.
- Discovery of an unlocked computer which is unattended must be reported via Peak Collections's Incident Reporting procedures.

PASSWORD DISCLOSURES:

- Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation – initially through the individual's line manager. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, the MD must be notified through Peak Collections's Incident Reporting procedures. For more information, Peak Collections Password policy is available on the intranet or via the line manager. Under no circumstances should an employee allow another employee to use their user account details after they have logged onto a system – even under supervision.

VIRUS WARNINGS/ALERTS:

- All Desktop, laptop and tablet computers in use across Peak Collections have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to Peak Collections data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to the MD as soon as possible, including a screenshot of any messages if possible.

MEDIA LOSS:

- Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data is generally prohibited. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any authorised user of a portable device who has misplaced or suspects damage, theft whether intentional or accidental of any portable media must report it immediately through Peak Collections's Incident Reporting procedures.

DATA LOSS/DISCLOSURE:

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised -recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on Peak Collections's website and identified as inaccurate or inappropriate (which must be reported)
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function Devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All Peak Collections employees, partner agencies, contractors and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Peak Collections data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using Peak Collections's Incident Reporting procedures

PERSONAL INFORMATION ABUSE:

- All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc… must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.
- Any abuse/misuse of such person identifiable information must be reported through Peak Collections's Incident Reporting procedures.

Physical Security:

- Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower floor/level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the IT Service via Peak Collections's Incident Reporting procedures.

- Continuing emphasis and re-enforcement of Peak Collections's Secure Desk policy will further help to reduce the number of security incidents.

LOGICAL SECURITY / ACCESS CONTROLS:

- Controlling, managing and restricting access to the Peak Collections's Network, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorized employees can gain access to information which is processed and maintained electronically.

MISSING CORRESPONDENCE:

- Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc… must be reported through Peak Collections's Incident Reporting procedures.

FOUND CORRESPONDENCE/MEDIA:

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, must be reported through Peak Collections's Incident Reporting procedures.

LOSS OR THEFT OF IT/INFORMATION:

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc… or which is known/or suspected to have been stolen needs to be reported immediately through Peak Collections's Incident Reporting procedures.

RESPONSIBILITIES:

It is the responsibility for all Peak Collections employees, partner agencies, contractors and vendors who undertake work for Peak Collections, on or off the premises to be proactive in the reporting of security incidents. Peak Collections's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of Peak Collections data and information.

It is also a responsibility of all individuals and handlers of Peak Collections data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

COMPLIANCE WITH LEGAL AND CONTRACTUAL OBLIGATIONS:

The Data Protection Act (2018) requires that personal data be kept secure against unauthorised access or disclosure.
The Computer Misuse Act (1990) covers unauthorised access to computer systems.

BREACHES OF POLICY:

- Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to Peak Collections assets, including IT equipment and information, or conduct which is in breach of Peak Collections's security procedures and policies.

- All Peak Collections employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through Peak Collections's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of Peak Collections.
- In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of Peak Collections's ICT systems or network results from the non-compliance, Peak Collections will consider legal action against the third party. Peak Collections will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under Peak Collections's disciplinary process.

- This Policy is referenced by other Peak Collections policies and guidelines. Copies of these policy statements are obtainable via Peak Collections's Intranet or by request to the IT Daprtment, as appropriate.
- This Policy is maintained and reviewed by Peak Collections's Security/Business Continuity Team and ratified by Peak Collections's senior management.

Acknowledgement:

I have read and understood the content of this policy.

I am aware of where to find it on the Integrated Management System to ensure I am updated with any amendments to it.

I agree to abide by the content of this policy at all times.

Signature:	Date: