Appendix 17 to
DUNCAN'S Minibus
Policy
& Code of Practice for
the Safe Use of
Minibuses
Dated: 30 May 2018

Duncan Private Hire Information/IT Security Policy

Policy
It is the policy of Duncan's Travel that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 6 (six) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within Duncan's Travel

At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical

Scope

The scope of information security includes the protection of the confidentiality, integrity and availability of information

The framework for managing information security in this policy applies to all Duncan's Travel entities and workers, and other Involved Persons and all Involved Systems throughout Duncan's Travel as defined below in Information Security definitions

This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in Information Classification

Risk Management

A thorough analysis of all Duncan's Travel information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource

The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level

Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities

Information Security Definitions

Affiliated Covered Entities: Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity

Availability: Data or information is accessible and usable upon demand by an authorized person

Confidentiality: Data or information is not made available or disclosed to unauthorised persons or processes

Integrity: Data or information has not been altered or destroyed in an unauthorised manner
Involved Persons: Every worker at Duncan's Travel, no matter what their status. This includes physicians, residents, students, employees, contractors, consultants, temporaries, volunteers, etc

Involved Systems: All computer equipment and network systems that are operated within the Duncan's Travel environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems
Protected Health Information (PHI): PHI is health information, including demographic information, created or received by the Duncan's Travel entities which relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and that identifies or can be used to identify the individual

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources

Information Security Responsibilities

Information Security Officer: The Information Security Officer (ISO) for each entity is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of

Duncan's Travel. Specific responsibilities include:

Ensuring security policies, procedures, and standards are in place and adhered to by entity

Providing basic security support for all systems and users

Advising owners in the identification and classification of computer resources. See Information Classification

Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation

Educating custodian and user management with comprehensive information about security controls affecting system users and application systems

Providing on-going employee security education

Performing security audits

Reporting regularly to Duncan's Travel on status with regard to information security Information Owner: The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an Organisational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual. The owner of information has the responsibility for:

Knowing the information for which she/he is responsible

Determining a data retention period for the information, relying on advice from a Legal Department

Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit

Authorizing access and assigning custodianship

Specifying controls and communicating the control requirements to the custodian and users of the information

Reporting promptly to the ISO the loss or misuse of Duncan's Travel information. Initiating corrective actions when problems are identified

Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate

Following existing approval processes within the respective Organisational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information

Custodian: The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

Providing and/or recommending physical safeguards

Providing and/or recommending procedural safeguards

Administering access to information

Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information

Evaluating the cost effectiveness of controls

Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO

Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate

Reporting promptly to the ISO the loss or misuse of Duncan's Travel information.

Identifying and responding to security incidents and initiating appropriate actions when problems are identified

User Management:

Duncan's Travel management who supervise users as defined below.

User management is responsible for overseeing their employees' use of information, including:

Reviewing and approving all requests for their employees access Authorisations

Initiating security change requests to keep employees' security record current with their positions and job functions

Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures

Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc

Providing employees with the opportunity for training needed to properly use the computer systems

Reporting promptly to the ISO the loss or misuse of Duncan's Travel information

Initiating corrective actions when problems are identified

Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information

User:
The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

Access information only in support of their authorized job responsibilities

Comply with Information Security Policies and Standards and with all controls established by the owner and custodian

Keep personal authentication devices (e.g. passwords, Secure Cards, PINs, etc.) confidential

Report promptly to the ISO the loss or misuse of Duncan's Travel information

Initiate corrective actions when problems are identified

Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format.

The following levels are to be used when classifying information:

Protected Health Information (PHI)

PHI is information, whether oral or recorded in any form or medium, that:
Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or health clearinghouse; and relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and Includes demographic data, that permits identification of the individual or could reasonably be used to identify the individual unauthorised or improper disclosure, modification, or destruction of this information could violate UK laws, result in civil and criminal penalties, and cause serious damage to Duncan's Travel and its patients or research interests

Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as PHI. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access

Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys

Unauthorised disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Duncan's Travel, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner

Internal Information

Internal Information is intended for unrestricted use within Duncan's Travel, and in some cases within affiliated organizations such as Duncan's Travel business partners. This type of information is already widely-distributed within Duncan's Travel, or it could be so distributed within the organization without advance permission from the information owner

Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages

Any information not explicitly classified as PHI, Confidential or Public will, by default, be classified as Internal Information

Unauthorised disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions

Public Information

Public Information has been specifically approved for public release by a designated authority within each entity of Duncan's Travel. Examples of Public Information may include marketing brochures and material posted to Duncan's Travel entity internet web pages This information may be disclosed outside of Duncan's Travel

Computer and Information Control

All involved systems and information are assets of Duncan's Travel and are expected to be protected from misuse, unauthorised manipulation, and destruction. These protection measures may be physical and/or software based

Ownership of Software: All computer software developed Duncan's Travel employees or contract personnel on behalf of Duncan's Travel or licensed for Duncan's Travel use is the property of Duncan's Travel and must not be copied for use at home or any other location, unless otherwise specified by the license agreement

Installed Software: All software packages that reside on computers and networks within Duncan's Travel must comply with applicable licensing agreements and restrictions and must comply with Duncan's Travel acquisition of software policies

Virus Protection: Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems

Access Controls: Physical and electronic access to PHI, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by Duncan's Travel. Mechanisms to control access to PHI, Confidential and Internal information include (but are not limited to) the following methods:

Authorisation: Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc

Role-based access: An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role

User-based access: A security mechanism used to grant users of a system access based upon the identity of the user

Identification/Authentication: Unique user identification (user id) and authentication is required for all systems that maintain or access PHI, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id

At least one of the following authentication methods must be implemented:

Strictly controlled passwords (Attachment 1 – Password Control Standards),
Biometric identification, and/or tokens in conjunction with a PIN

The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager

An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes)

The user must log off or secure the system when leaving it

Data Integrity: Duncan's Travel must be able to provide corroboration that PHI, Confidential, and Internal Information has not been altered or destroyed in an Unauthorised manner.

Listed below are some methods that support data integrity
:
Transaction audit
Disk redundancy (RAID)
ECC (Error Correcting Memory)
checksums (file integrity)
Encryption of data in storage
Digital signatures

Transmission Security: Technical security mechanisms must be put in place to guard against unauthorised access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

Integrity controls and encryption, where deemed appropriate

Remote Access: Access into Duncan's Travel network from outside will be granted using Duncan's Travel approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, PHI, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the Duncan's Travel network

Physical Access: Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals

The following physical controls must be in place:

Mainframe computer systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations
File servers containing PHI, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorised individuals
Workstations or personal computers (PC) must be secured against use by unauthorised individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:
Position workstations to minimize unauthorised viewing of protected health information

Grant workstation access only to those who need it in order to perform their job function
Establish workstation location criteria to eliminate or minimize the possibility of unauthorised access to protected health information

Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to PHI

Use automatic screen savers with passwords to protect unattended machines

Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

Contingency Operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency

Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorised physical access, tampering, and theft

Access Control and Validation – Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision

Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks)

Emergency Access:

Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

Procedures must be documented to address:

Authorisation, Implementation, and Revocation

Equipment and Media Controls: The disposal of information must ensure the continued protection of PHI, Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility.

The following specification must be addressed:

Information Disposal / Media Re-Use of:
Hard copy (paper and microfilm/fiche)
Magnetic media (floppy disks, hard drives, zip disks, etc.) and CD ROM Disks
Accountability: Each entity must maintain a record of the movements of hardware and electronic media and any person responsible therefore
Data backup and Storage: When needed, create a retrievable, exact copy of electronic PHI before movement of equipment

Other Media Controls:

PHI and Confidential Information stored on external media (diskettes, cd-roms, portable storage, memory sticks, etc.) must be protected from theft and unauthorised access. Such media must be appropriately labeled so as to identify it as PHI or Confidential Information. Further, external media containing PHI and Confidential Information must never be left unattended in unsecured areas

PHI and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:

Power-on passwords
Auto logoff or screen saver with password
Encryption of stored data or other acceptable safeguards approved by Information Security Officer
Further, mobile computing devices must never be left unattended in unsecured areas
If PHI or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of Duncan's Travel Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with Duncan's Travel

Data Transfer/Printing:

Electronic Mass Data Transfers: Downloading and uploading PHI, Confidential, and Internal Information between systems must be strictly controlled. Requests for mass downloads of, or individual requests for, information for research purposes that include PHI must be approved and include only the minimum amount of information necessary to fulfill the request.

Other Electronic Data Transfers and Printing: PHI, Confidential and Internal Information must be stored in a manner inaccessible to unauthorised individuals. PHI and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PHI that is downloaded for educational purposes where possible should be de-identified before use

Oral Communications: Duncan's Travel staff should be aware of their surroundings when discussing PHI and Confidential Information. This includes the use of cellular telephones in public areas. Duncan's Travel staff should not discuss PHI or Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation

Audit Controls: Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for six (6) years

Evaluation: Duncan's Travel requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection

Contingency Plan: Controls must ensure that Duncan's Travel can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PHI, Confidential, or Internal Information.

Disaster Recovery Plan: A disaster recovery plan will be developed and documented to contain a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure

Emergency Mode Operation Plan: A plan will be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure

Testing and Revision Procedures: Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary

Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented

Compliance

The Information Security Policy applies to all users of Duncan's Travel information including: employees, medical staff, students, volunteers, and outside affiliates. Failure to comply with Information Security Policies and Standards by employees, medical staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Duncan's Travel procedures, or, in the case of outside affiliates, termination of the affiliation. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

Unauthorised disclosure of PHI or Confidential Information as specified in Confidentiality Statement

Unauthorised disclosure of a sign-on code (user id) or password

Attempting to obtain a sign-on code or password that belongs to another person

Using or attempting to use another person's sign-on code or password

Unauthorised use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review

Installing or using unlicensed software on Duncan's Travel computers

The intentional unauthorised destruction of Duncan's Travel information

Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access

--- ATTACHMENT 1 ---

Password Control Standards

The Duncan's Travel Information Security Policy requires the use of strictly controlled passwords for accessing Protected Health Information (PHI), Confidential Information (CI) and Internal Information. (See Duncan's Travel Information Security Policy for definition of these protected classes of information.)

Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls

Standards for accessing PHI, CI,:

Users are responsible for complying with the following password standards:

Passwords must never be shared with another person, unless the person is a designated security manager

Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity of the information being accessed)

Passwords must, where possible, have a minimum length of six characters

Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems

Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them

When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc…). A combination of alpha and numeric characters are more difficult to guess

Where possible, system software must enforce the following password standards:

Passwords routed over a network must be encrypted.

Passwords must be entered in a non-display field

System software must enforce the changing of passwords and the minimum length

System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15 minute timeframe. Lockout time must be set at a minimum of 30 minutes

System software must maintain a history of previous passwords and prevent their reuse