Appendix 17
DUNCAN'S Minibus Policy
Safe Use of Minibuses
Date: 14 May 2025

Duncan Private Hire
Information & IT Security Policy

Policy Overview

Duncan Private Hire is committed to protecting all forms of information—whether written, verbal, electronic, or printed—from accidental or unauthorized alteration, destruction, or disclosure throughout its entire lifecycle. This protection extends to the hardware and software used to process, store, and transmit such information, ensuring robust security measures are in place at all times.

All related policies and procedures must be documented, accessible to those responsible for their enforcement, and activities governed by these policies must also be recorded. Documentation—whether electronic or physical—will be retained for a minimum of six years following its creation or update. Regular reviews will ensure all policies remain current and appropriate, with review intervals set by each department within Duncan Private Hire.

Each department or entity within Duncan Private Hire may develop specific policies and procedures tailored to their operational needs, provided they align with this overarching policy. New systems must comply with these standards from implementation; existing systems will be updated to meet compliance as feasibly and promptly as possible.

Scope

This policy safeguards the confidentiality, integrity, and availability of all information assets across Duncan Private Hire. It applies to all employees, contractors, volunteers, and any personnel with access to Duncan Private Hire systems and data ("Involved Persons"). It covers all hardware, software, networks, and data ("Involved Systems") utilized within the organization.

The policy governs all protected health information (PHI) and other sensitive data types as defined by Duncan Private Hire's classification standards.

Risk Management

Periodic comprehensive risk assessments will be conducted to identify threats and vulnerabilities affecting Duncan Private Hire's information systems. These assessments will cover:

- Internal and external risks, including natural, human, electronic, and non-electronic threats.
- Existing vulnerabilities that may expose information assets.
- Evaluation of assets and technology supporting data collection, storage, and dissemination.

The combined analysis will estimate risks to the confidentiality, integrity, and availability of information. Each entity will determine the frequency of these assessments. Based on

findings, appropriate mitigation strategies will be implemented to minimize vulnerabilities and protect critical information assets.

Key Definitions

- Affiliated Covered Entities: Legally separate entities that operate collectively under a unified compliance framework.
- Availability: Authorized personnel can access information when needed.
- Confidentiality: Information is protected from unauthorized access or disclosure.
- Integrity: Information remains accurate and unaltered except through authorized means.
- Involved Persons: All workers within Duncan Private Hire, including employees, contractors, volunteers, and temporary staff.
- Involved Systems: All IT equipment, platforms, applications, and data used within Duncan Private Hire.
- Protected Health Information (PHI): Individually identifiable health information related to an individual's medical history, treatment, or payment for healthcare services.
- Risk: The likelihood of compromise to confidentiality, integrity, or availability of information assets.

Roles & Responsibilities

Information Security Officer (ISO):

- Develops, implements, and enforces security policies and controls in collaboration with management.
- Provides security support, advice, and education across the organization.
- Oversees security audits and reports regularly on security status.
- Advises on classification, protection, and handling of information assets.
- Leads ongoing staff education on information security best practices.

Information Owner:

- Typically a manager responsible for information creation or primary usage.
- Defines data retention schedules in consultation with legal advisors.
- Ensures controls to maintain confidentiality, integrity, and availability.
- Authorizes access and delegates custodianship.
- Communicates security requirements and reports incidents promptly.
- Supports staff training and awareness initiatives.
- Oversees system procurement and implementation approval processes.

Information Custodian:

- Manages day-to-day handling, processing, and storage of information.
- Implements physical and procedural safeguards as directed by the owner.
- Controls access and ensures authorized information release.
- Collaborates with the ISO and owners to maintain secure information environments.

Continued: Custodian Responsibilities

- Releasing information as authorised by the Information Owner and/or the Information Privacy/Security Officer, following procedures that ensure data privacy.
- Evaluating the cost-effectiveness of proposed or existing controls.

- Maintaining current and relevant information security policies, procedures, and standards, in coordination with the ISO.
- Promoting employee awareness and education through ISO-approved programs.
- Promptly reporting any loss, breach, or misuse of Duncan Private Hire information to the ISO.
- Identifying and responding to security incidents and initiating timely corrective actions.

User Management Responsibilities

User management includes any Duncan Private Hire personnel who oversee or supervise employees, contractors, or others with access to company systems.

Managers are responsible for:

- Reviewing and approving access requests for their staff.
- Initiating updates to user access rights when roles or job functions change.
- Promptly notifying relevant teams of employee terminations or transfers and enforcing local offboarding protocols.
- Ensuring revoked employees are denied physical access—this includes collecting access cards, keys, and updating lock combinations where applicable.
- Providing employees with appropriate training on the secure and efficient use of IT systems.
- Reporting any suspected or known misuse of information to the ISO.
- Initiating corrective actions upon identifying security issues.
- Following internal approval processes for the procurement or deployment of new software or systems.

User Responsibilities

A user is any individual who is authorised to read, input, or modify Duncan Private Hire information.

Users are expected to:

- Access data solely in alignment with their job responsibilities.
- Comply with all Information Security Policies, procedures, and specific controls established by the data owner or custodian.
- Keep personal authentication mechanisms (e.g., passwords, security tokens, PINs) secure and confidential.
- Immediately report any actual or suspected data breach, loss, or misuse to the ISO.
- Participate in corrective measures when security issues are identified.

Information Classification

Information classification helps ensure appropriate security controls are applied based on data sensitivity. All information must be protected for its integrity and accuracy, regardless of classification.

Classification is determined based on the most sensitive element of the data and applies across all formats (physical, digital, oral).

Classification Levels:

1. Protected Health Information (PHI):
Data that identifies or could reasonably identify an individual, relating to their physical or mental health, the provision of healthcare, or payment for healthcare services.
Examples include medical records, treatment history, insurance data, and associated demographics.

- **Risks:** Improper use or disclosure may breach UK data protection laws and result in legal, financial, and reputational damage.

2. Confidential Information:
Highly sensitive data not classified as PHI, including personnel records, financial data, access credentials, and proprietary research.
Access must be strictly controlled and limited to those with a legitimate business need.

- **Risks:** Unauthorized access may violate regulations or harm business interests.

3. Internal Information:
Data intended for use within Duncan Private Hire and its affiliates. While not highly sensitive, its distribution outside the organisation may still be inappropriate.

- **Examples:** Internal emails, operational policies, non-public reports.

4. Public Information:
Information explicitly approved for external release by an authorised party.

- **Examples:** Public websites, brochures, press releases.

Computer and Information Control

All systems, hardware, software, and data used or managed within Duncan Private Hire are considered company assets and must be protected against unauthorised access, tampering, or destruction.

Software Ownership & Usage

- All software developed or procured on behalf of Duncan Private Hire is company property and may not be copied or used outside the organisation unless expressly permitted by a license agreement.
- All installed software must comply with licensing terms and company acquisition policies.

Virus Protection

- Duncan Private Hire enforces a multi-layered antivirus strategy—encompassing desktops, servers, and network gateways—approved by the ISO and IT Services.
- Users are prohibited from disabling or interfering with antivirus protection tools.
- All electronic files must be scanned prior to execution or storage.

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 (ISO) and approved by Duncan Private Hire.

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. Acceptable methods include:

- Context-based access: Access control based on transaction context such as time of day, location of the user, and strength of user authentication.
- Role-based access: Access rights are assigned to predefined roles, with users assigned one or more roles based on their job function.
- User-based access: Access is granted based on the individual user’s identity.

Identification / Authentication

Unique user identification (user ID) and authentication are required for all systems that access PHI, Confidential, or Internal Information.

Authentication methods must include at least one of the following:

- Strictly controlled passwords (see **Attachment 1 – Password Control Standards**)
- Biometric identification
- Tokens with PIN

Additional authentication controls:

- Authentication controls (passwords, tokens, etc.) must be known only to the user.
- Systems must automatically time out and require re-authentication after 15 minutes of inactivity.
- Users must log off or lock their systems when unattended.

Data Integrity

Duncan Private Hire must corroborate that PHI, Confidential, and Internal Information has not been altered or destroyed in an unauthorised manner. Examples of controls that support data integrity include:

- Transaction audits
- Disk redundancy (RAID)
- ECC (Error Correcting Memory)
- Checksums
- Encryption of stored data
- Digital signatures

Transmission Security

To prevent unauthorised access during transmission of data over communication networks (including wireless):

- Implement integrity controls and encryption where appropriate.
- Transmission must follow ISO-approved protocols and encryption standards.

Remote Access

- Remote access is permitted only through Duncan Private Hire-approved devices and secure pathways.
- PHI, Confidential, and Internal Information stored or accessed remotely must maintain the same level of protection as internal systems.
- Unauthorised remote access methods are strictly prohibited.

Physical Access

Access to information processing facilities is restricted to authorized personnel only.

Required controls:

- Mainframe and File Server Areas: Must be access-controlled and environmentally protected.
- Workstations/PCs: Must prevent unauthorised viewing or access.
    - Position screens away from public view
    - Use secure workstation location criteria
    - Enable auto screen savers with passwords
- Facility Access Controls:
    - Contingency Operations: Facility access procedures during emergencies
    - Facility Security Plan: Safeguard facility and equipment from physical threats
    - Access Control and Validation: Validate facility access based on user roles
    - Maintenance Records: Document physical facility security changes

Emergency Access

Mechanisms must be in place to allow access to systems and applications during emergencies when assigned custodians are unavailable.

Procedures must document:

- Authorisation
- Implementation
- Revocation

Equipment and Media Controls

Policies must govern the secure handling, disposal, and movement of electronic media containing PHI and other sensitive information.

- Disposal/Reuse: Secure disposal of:
    - Paper
    - Magnetic Media (floppy disks, hard drives, zip disks)
    - CD-ROMs
- Accountability: Maintain logs of media movement and custodianship

- Data Backup: Back up PHI prior to equipment movement

Media and Mobile Device Controls

- External media containing PHI/Confidential Information must be labeled and secured.
- Mobile devices must have:
  - Power-on passwords
  - Auto logoff/screen saver with password
  - Encrypted storage
- Devices must not be left unattended in unsecured areas.
- Breaches due to mishandling of mobile devices or media will result in personal accountability.

Data Transfer / Printing

- Mass Transfers: Requests involving PHI must be approved and include the minimum necessary data.
- Printing: PHI/Confidential data must be printed only when necessary and safeguarded.
- De-identification: Where possible, PHI should be de-identified for educational/research use.

Oral Communications

Staff must avoid discussing PHI or Confidential Information in public or semi-public areas. Use discretion when using cell phones or communicating near:

- Waiting areas
- Hallways
- Elevators
- Public transportation

Audit Controls

Mechanisms must be in place to log and review access to systems that use or store PHI. These audit records must be:

- Reviewed regularly
- Retained for six (6) years
- Used to track security incidents and unauthorized activity

Evaluation

Periodic evaluations must be conducted in response to environmental or operational changes to ensure ongoing protection of electronic PHI and alignment with current standards.

Contingency Plan

Each entity must prepare to recover from damage to IT systems or data loss.

Components include:

- Disaster Recovery Plan: Restore data after disasters
- Emergency Mode Operation Plan: Continue operations during adverse events
- Testing and Revision: Periodically test and revise contingency plans
- Applications and Data Criticality Analysis: Assess and document system/data importance

Compliance

This policy applies to all users of Duncan Private Hire information, including employees, contractors, volunteers, and affiliates. Violations may result in:

- Disciplinary actions (including termination)
- Loss of affiliation
- Legal consequences (for breaches of PHI or confidentiality)

Violations include but are not limited to:

- Unauthorised access or disclosure of PHI/Confidential Information
- Sharing or misusing passwords or user credentials
- Using or installing unauthorised software
- Tampering with or destroying information intentionally

Attachment 1 – Password Control Standards

Minimum password standards for access to PHI, Confidential, and Internal Information:

- Passwords must not be shared (except with designated security managers)
- Change frequency: 45–90 days based on data sensitivity
- Minimum length: 6 characters
- Passwords must not be auto-saved (except approved SSO)
- Avoid dictionary or guessable words (e.g., pets' names, birthdays)
- Use alphanumeric combinations

System-enforced standards must include:

- Encrypted password transmission
- Password input hidden (non-display fields)
- Lockout after 3 failed attempts in 15 minutes (30-minute lockout)
- Password history tracking to prevent reuse

.