Plan Overview

A Data Management Plan created using DMPonline

Title: Developing Practical Cybersecurity Readiness Guidance for Hong Kong Logistics and Grocery Retail SMEs

Creator: Chamber Lain Law

Principal Investigator: Law Chamber Lain

Data Manager: Law Chamber Lain

Project Administrator: Law Chamber Lain

Contributor: Rong Huang

Affiliation: University of Plymouth

Template: DCC Template

Project abstract:

This project will develop and evaluate a practical cybersecurity readiness guidance pack for Hong Kong logistics and grocery retail small and medium-sized enterprises (SMEs). The pack will include a Computer System Security Management Plan and an Emergency Response Plan. It aims to help companies identify critical digital services and dependencies, prioritise proportionate preventive and detective actions, assign responsibilities, and prepare for cyber-incident response and recovery. The project will use documentary review and confidential interviews with SME decision-makers, IT personnel and external providers to identify user needs and translate them into design requirements. Version 1 will then be evaluated through scenario-based tasks for clarity, usefulness, relevance, feasibility and governance fit. The project does not provide legal advice, certify compliance or implement controls for participating companies. Instead, it will provide an editable guidance pack that companies can use as a reference for later internal feasibility and adoption decisions.

ID: 213499

Start date: 03-11-2026

End date: 31-03-2027

Last modified: 25-10-2026

Copyright information:

The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customise it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan's text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal

Developing Practical Cybersecurity Readiness Guidance for Hong Kong Logistics and Grocery Retail SMEs

Data Collection

What data will you collect or create?

The project will collect consent forms, participant contact details, eligibility-screening information, interview recordings where separately consented, agreed interview notes where recording is not used, anonymised transcripts or summaries, translation notes for Cantonese material, researcher reflexive memos, and evaluation-task records. It will also create an evidence register, alternatives matrix, requirements matrix, anonymised thematic codes, a Version 1 cybersecurity readiness guidance pack, an evaluation record and a future-enhancement register. No passwords, IP addresses, network diagrams, exploitable configurations, unpatched vulnerabilities, customer data or identifiable live-incident details will be requested or retained.

How will the data be collected or created?

Data will be collected through documentary review and approximately 45–60-minute semi-structured interviews with SME owners, managers, operational decision-makers, internal IT staff and external IT or security providers. Version 1 will be evaluated through individual scenario-based sessions using fictional logistics or grocery retail cases. Interviews will be conducted in English or Cantonese after ethical approval and informed consent. Audio recording will occur only with separate consent; otherwise, agreed notes will be used. Cantonese materials will be retained in the original language, and translation decisions will be documented.

Documentation and Metadata

What documentation and metadata will accompany the data?

Each research file will use a unique participant or document code rather than a company or personal name. A data inventory will record file name, date, file type, version, source, language, consent status, anonymisation status, access restrictions and retention/deletion date. A data dictionary will define codes, abbreviations and fields used in the evidence register, requirements matrix and evaluation record. Version control will be used for the guidance pack and associated design decisions.

Ethics and Legal Compliance

How will you manage any ethical issues?

University ethical approval will be obtained before recruitment, interviewing or evaluation. Participants will receive an information sheet and provide informed consent. Participation is voluntary. Participants have the right to withdraw within two weeks of their session, or before their data are anonymised and aggregated (anticipated by mid-January 2027), after which individual data can no longer be identified or withdrawn. This will be clearly communicated in the Participant Information Sheet. Contact details and consent forms will be stored separately from research data. Reporting will use anonymised and aggregated findings; no company-specific weakness, gap or vulnerability will be disclosed in a way that could create a targeting opportunity. The study will avoid collecting sensitive cyber-security information and will use fictional scenarios for evaluation where possible.

How will you manage copyright and Intellectual Property Rights (IPR) issues?

The project will use publicly available reports, standards overviews and guidance materials lawfully and will cite all sources. Copyrighted standards or guidance will not be reproduced beyond what is permitted for academic citation and analysis. Participants retain ownership of information about their organisations; the researcher will use only the information they voluntarily provide under

informed consent. The Version 1 guidance pack and project outputs will be managed according to University of Plymouth policies and the assessment requirements.

Storage and Backup

How will the data be stored and backed up during the research?

Digital research data will be stored in encrypted, password-protected University-approved storage or another University-approved secure location. Working files will be backed up through the approved institutional service. Contact details and consent records will be held separately from coded interview, evaluation and analysis files. Personal devices will not be the sole storage location for research data. Any temporary local copies will be encrypted and removed once securely transferred.

How will you manage access and security?

Access will be restricted to the student researcher and, where required for academic supervision or assessment, authorised University staff. Strong passwords, multi-factor authentication where available and device screen locking will be used. Files containing identifiable data will have the highest access restriction. Data shared with a supervisor will be anonymised wherever feasible and transferred only through University-approved systems.

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved?

Research data will be retained and deleted in accordance with the University of Plymouth's Research Data Policy. Anonymised research data will be retained follow the university policy instead of dictate by researcher in approvved institutional storage. Identifiable data will be securely destroyed once no longer required for the assessment process (anticipated by July 2027) or upon valid withdrawal request. No sensitive cyber-security information will be preserved as a reusable dataset.

What is the long-term preservation plan for the dataset?

Research data will be retained and deleted in accordance with the University’s approved ethics, assessment and retention requirements. The final anonymised project outputs will be retained only for the required period and in approved institutional storage. Identifiable data will be securely destroyed when no longer required under the approved retention schedule. No sensitive cyber-security information will be preserved as a reusable dataset.

Data Sharing

How will you share the data?

The final summative proposal and Version 1 guidance pack may be shared with the University for assessment. Only anonymised, aggregated findings may be included in academic work or future presentation. The project will not publish raw interview recordings, consent forms, contact details, detailed transcripts or company-specific evaluation records.

Are any restrictions on data sharing required?

Yes. Raw and identifiable research data will be restricted because it may contain personal information, commercially sensitive context or cyber-security-related information. Even anonymised material will be reviewed before sharing to ensure that it cannot identify a participant, company, supplier or security weakness. Any sharing outside the University will require appropriate consent, ethical approval and University permission.

Responsibilities and Resources

Who will be responsible for data management?

Law Chamber Lain, as the student researcher and Principal Investigator, will be responsible for collecting, organising, anonymising, securing, backing up, retaining and deleting research data. The academic supervisor may provide oversight but will not be responsible for routine data handling unless required by University procedures.

What resources will you require to deliver your plan?

The project requires University-approved encrypted storage, a password-protected computer, secure University email or approved file-transfer tools, word-processing and spreadsheet software, transcription and translation support where necessary, and sufficient time to anonymise, organise and securely delete data. No specialised live-system access, security-testing tools or company network access are required.