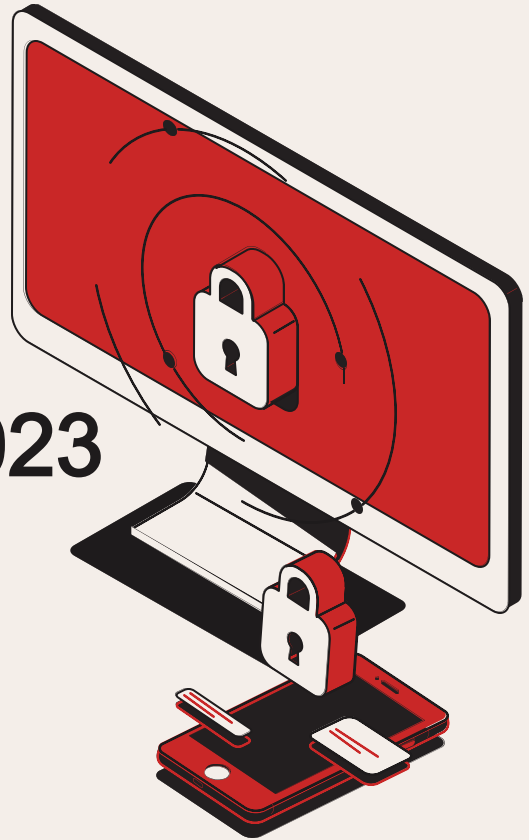
# Experience Sharing Session on Good Data Governance by Privacy-Friendly Awardees 2023



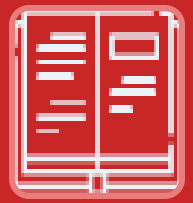

Speaker
Ms. Kaisy HUNG
Senior Statistician (Information Technology Services and Infrastructure)
Census and Statistics Department

# Introduction

- No single measure can effectively ensure personal data protection
- In order to safeguard personal data security, the Census and Statistics Department (C&SD) has adopted the approach of multiple layers of defense

# Privacy Management Programme – Organisational Commitment

- Top-down approach to foster a respectful culture for personal data privacy
- Ongoing review of the privacy management programme



Implement 16 recommendations made by the **Working Group on Review of Security Measures and Procedures for Handling the Data Collected from Respondents** to further enhance the data security measures and procedures in short, medium and long-term

Set up the **Departmental Committee on Data Security of Statistical Systems (DCDSSS)** to direct the departmental data security policies and oversee the ongoing development and implementation of recommendations on data security

# Privacy Management Programme –
## Departmental Committee on Data Security of Statistical Systems (DCDSSS)

- Chaired by the Deputy Commissioner with 10+ members from different grades
- Regularly reviews C&SD's data security measures to formulate data security plans and comprehensive guidance in terms of

Policies and procedures

Use of technology

Promotion of staff awareness

# Use of Technology
# - Data Anonymisation Module (DAM)

Protect private or sensitive information by encrypting identifiers in the dataset after data collection, without affecting the overall efficiency

The identifiers will be replaced by randomly generated series of letters / numbers (hash identifiers) and securely kept in the system

The hash identifiers can be used to differentiate records in the anonymous dataset and act as keys for data matching

The personal data cannot be identifiable from the anonymous dataset and only authorised officers can retrieve the original identifiers through the system for operational needs

# Use of Technology
# - Online Questionnaire System (OQS)

## Data encryption

- Use the Transport Layer Security (TLS) protocol to securely transmit data between clients and servers
- Store the submitted data in an encrypted form, without storage on users' computers

## User authentication

- Verify user identity for each login
- Lock the user account after a number of unsuccessful login attempts

## IT infrastructure

- Protect all servers by firewall
- Set up monitoring facilities to prevent unauthorised access

## Housekeeping

- Housekeep by deleting the expired user accounts and survey data

# Use of Technology - Mobile Tablets for Data Collection

### Data encryption and upload

- Encrypt collected data immediately and upload to central server
- Delete data from the tablets after uploading

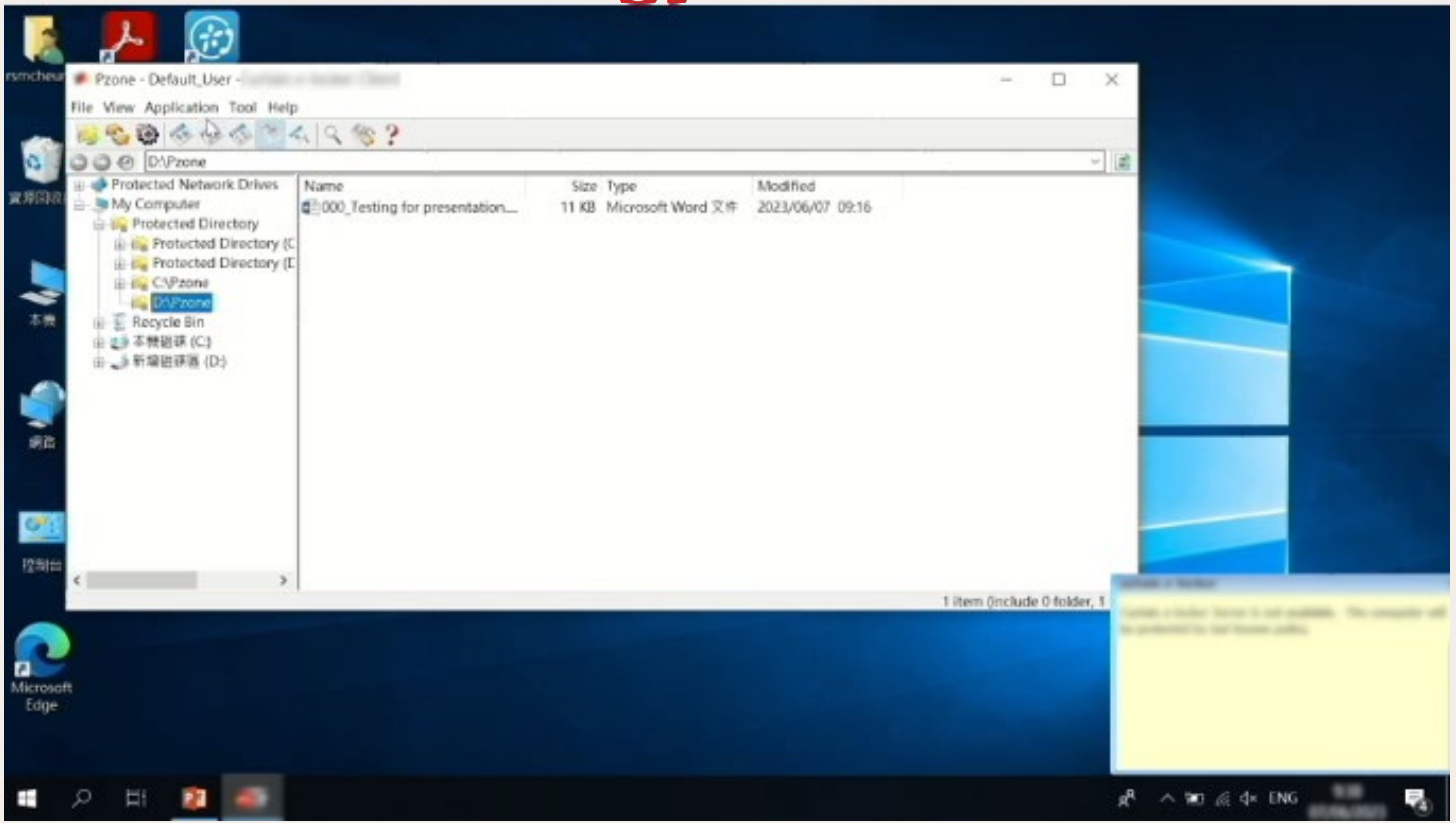
### Dual authentication

- Enable the power-on login and password-protected screen savers
- Adopt system login authentication with verification of server certificates

### Device management to deal with suspected loss of tablet

- Use Mobile Device Management (MDM) software to manage control and track the status of tablet
- Remotely delete all data on the tablet

# Use of Technology - Protected Zone



# Conclusions

- Technological advancements have brought convenience and opportunities to government statistical work, but also pose challenges to personal data protection

- To establish a robust personal data privacy management system, it is essential to have stringent policies and procedures, support of technological infrastructure, and ongoing education and staff training

# Thank you!