創新科技及工業局

香港添馬添美道二號
政府總部西翼二十樓

Innovation, Technology and Industry Bureau

20/F West Wing, Central Government Offices,
2 Tim Mei Avenue, Tamar, Hong Kong

本函檔號 Our Ref.: ITIB/POL/200/15/2(O)Pt.11
來函編號 Your Ref: CB(1)565/2024(01)
電話 Tel: 3655 4787
圖文傳真 Fax 2702 6036

By Email

Panel on Information Technology and Broadcasting Secretariat
Legislative Council
Legislative Council Complex,
1 Legislative Council Road,
Central, Hong Kong
(Attn.: Mr Daniel SIN)

Mr Sin,

Information System Security of Government and Public Organisation

I refer to Hon Michael TIEN's letter dated 6 May 2024 to the Chairman of the Panel, Hon Elizabeth QUAT concerning the security of information systems of government and public bodies, the engagement of contractors and the mechanism to monitor their performance, as well as the protection of personal data privacy. In consultation with the Office of the Government Chief Information Officer (OGCIO), the Constitutional and Mainland Affairs Bureau (CMAB) and the Office of the Privacy Commissioner for Personal Data (PCPD), our reply is as follows:

Strengthening information and cyber security

The Government is very concerned about the recent information system security incidents involving individual government departments and public bodies. These incidents show that bureaux and departments (B/Ds) as well as all sectors of society must stay vigilant about information and cyber security risks at all times, enhance security awareness, and strengthen the protection of information technology systems and data.

All B/Ds shoulder the responsibility of the first line of defence to ensure the primary security of their information technology (IT) systems and data, while OGCIO (and the future Digital Policy Office) plays a supervisory role through formulation of policies and operational practices for regulatory and cyber security matters, providing appropriate guidance and technical support to B/Ds, and enhancing B/Ds' ability to monitor the implementation

of IT systems and the protection of system and data security within their purview and that of their related public bodies.

OGCIO has formulated and updated from time to time the "Government Information Technology Security Policy and Guidelines" (Policy and Guidelines), which covers the information security management framework, policies and measures for B/Ds to comply with and adopt. The Policy and Guidelines is also published for reference by the industry (including both public and private organisations) and their formulation of appropriate IT security measures having regard to their own situations.

Under the existing Policy and Guidelines, B/Ds are directly responsible for the implementation and security of their IT projects. The scope of their main responsibilities include the following:

1. Comply with and adopt the information security risk management system, technical requirements and reference standards as stated in the Policy and Guidelines;

2. Supervise the implementation of their IT systems and ensure that relevant personnel adhere to the Policy and Guidelines;

3. Conduct regular security risk assessments and audits (SRAA) for their IT infrastructure, information systems and data assets;

4. Conduct privacy impact assessment (PIA) during the information system design stage and before launching updates that may have significant impacts;

5. Report information security incidents to the Government Information Security Incident Response Office, and notify as appropriate the PCPD and/or the Police depending on the nature of incident; and

6. Government officers should strictly follow the other applicable rules and regulations, including the Security Regulations, the Official Secrets Ordinance and the Civil Service Code.

Government B/Ds must comply with the requirements set out in the Policy and Guidelines. The relevant information security principles are generally in line with the directions of the measures recommended in the Guidance Note on Data Security Measures for Information and Communications Technology issued by the PCPD, covering for example encryption of data during transmission and storage, prohibition against

storing sensitive and personal data on public cloud platforms, and conducting regular SRAA by B/Ds.

In order to strengthen the main supervisory role of B/Ds in government IT projects and to more effectively protect information systems and data security, OGCIO will further enhance the existing measures, including requiring B/Ds to appoint senior officers to closely oversee the security assessment of the information systems under their purview or public bodies subject to their supervision; closely monitoring the conduct of PIA; introducing regular testing; strengthening compliance audits of high-risk systems; conducting cyber security attack and defence drills; enhancing staff training; and improving the system security awareness and response capabilities of senior personnel.

Enhancing the tender and penalty mechanism for contractors

Government IT systems are based on the public services that individual departments provide. Hence, B/Ds will be responsible to initiate their IT projects, invite tenders and take forward the projects in accordance with their policies and requirements of their service clients.

To assist departments in managing and monitoring their IT service contractors, OGCIO has issued the Practice Guide to Project Management for IT Projects under an Outsourced Environment, covering project initiation, planning, implementation and completion. The Practice Guide also recommends a set of good practices for B/Ds to follow. B/Ds would monitor their contractors in accordance with the contract terms; if the performance of contractors fail to fulfil the service requirements and standards specified in the contracts, departments may take actions based on the contractual provisions. These actions include warning, demand for compensation or even early termination of contract.

On the other hand, OGCIO promulgated a series of new measures to all B/Ds in February this year. Among the measures, B/Ds are required to raise the weighting of technical assessments in tender-marking schemes to 70 per cent when procuring the system development services for large-scale or high-risk systems. The higher weighting of technical assessments helps B/Ds engage the most capable service contractors with suitable technical expertise, thereby improving the quality of IT projects.

For those smaller-scale projects with a budget not exceeding $20 million, OGCIO implements the Standing Offer Agreement for Quality Professional Services Scheme (the SOA-QPS Scheme) to facilitate their speedy implementation. Under the Scheme, B/Ds can directly invite contractors having passed OGCIO's pre-qualification to submit proposals for

B/Ds to select suitable service contractors. OGCIO can suspend those contractors with continuous subpar performance from further bidding under the SOA-QPS Scheme until their performance improves.

Protection of Personal Data Privacy

According to the Personal Data (Privacy) Ordinance (PDPO) (Cap. 486), any persons or organisations (including government departments, public bodies and private organisations) in their capacity of data users shall comply with the PDPO and its six Data Protection Principles during the collection, holding, processing or use of personal data.

The PCPD has been proactively relying on the powers conferred to PCPD under the PDPO to scrutinise the personal data breach incidents of organisations, as well as helping organistions handle such breach incidents and adopt improvement measures. Moreover, the PCPD has been utilising its powers of handling complaints and investigation to handle complaints on insufficient personal data security and notifications on data breach incidents. If following investigation data users are discovered to have contravened the PDPO, the Privacy Commissioner will issue enforcement notices where appropriate, directing data users to take remedial measures so as to rectify the contravention and prevent similar incidents from reoccurrence.

Thank you for comments from Members on the above matters.

Yours sincerely,

(Mr Arthur CHAN)
for Secretary of Innovation,
Technology and Industry

c.c.
Constitutional and Mainland Affairs Bureau
(Attn.: Mr Hansel WONG)
Office of the Government Chief Information Officer
(Attn.: Mr Daniel CHEUNG)