Government of Haryana/ हरियाणासरकार

Secretariat for Information Technology
सूचनाप्रौद्योगिकीसचिवालय

From

Secretary to Govt., Haryana
Electronics and Information Technology Department, Haryana
Government of Haryana

To

All the Administrative Secretaries,
Government of Haryana

No. Admn/194/1-SIT/6897 Date: 27 June 2018

Sub: Regarding the conformance of the contracts to the Information Technology Act, 2000

Sir,

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act 2000) among other subjects also dealswith cybercrime and electronic commerce and provides legal framework for electronic governance by giving recognition to electronic records. It also defines the scope of cyber related crimes and prescribed penalties for them.

In recent time, the incidents related to cybercrimes, cyber thefts have increased multi-folds which makes far more important for Government Departments to emphasize upon the importance of incorporating provisions of the aforementioned act in the contractsfor outsourcing services or procuring hardware/ software solutions or hiring developers for a customising a website or some software etc. These hired agencies/ SI/ developers, etc.gets secured access to the departmental, citizen and other important data and can misuse the same un-knowingly or intentionally which can harm the image and trust among the citizens.

Therefore, it is recommended that the:

a) Specific mention of the IT Act 2000 in the contracts/ agreements will empower the Departments/ Boards/ Corporations to act against the defaulters in the event of breach. The relevant sections of the Act are mentioned in the Annexure 'A' enclosed. Model clause that can be included in the contracts that departments sign with private service providers is also enclosed herewith. The Head SeMT/CISO may be contacted for any further clarifications in this regard. It is requested that the model clause be included in all future contractual agreements as well as previous contracts may also be revised and included afresh

b) Departments/ Boards/ Corporations setting their software/web applications, mobile applications etc. developed through outsourcing agencies/venders must include the requirement of security audit clearance certificate for the application from anyone of the registered CERT-In empanelled agencies and its annual renewal till the time of their engagement, as well

(Vijayendra Kumar)

Copy for kind information of:

1. PS to CS, Haryana for kind information of Chief Secretary, Haryana
2. PS to ACS E&IT for kind information of ACS E&IT

9th Floor, Haryana Civil Secretariat, Chandigarhनौवींमं जेल, हरियाणासिविलसचिवालय, चण्डीगढ़
Tel./दूरभाष:Secretary/सचिव: 0172-2704922, Fax/QSDI:0172-2705529
E-mail/ई–मेलmdhartron-hry@gov.in Website/वैबस ईट:www.haryanait.gov.in

CFMS No. 8889 Dated 05/07/18
O/o ACSTE

3. SIO NIC
4. Sh. Munish Chandan, Head SeMT/ Chief Information Security Officer (headsemtharyana@gmail.com), Landline no. 0172 -2703479
5. All MDs/CEOs of Boards/Corporation
6. All Departments
7. All Deputy Commissioners

Government of Haryana/ हरियाणासरकार
Secretariat for Information Technology
सूचनाप्रौद्योगिकीसचिवालय

Model Clauses for any IT Outsourcing Contract for Security & Safety

"Service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of Personal Information does and will comply with all applicable privacy and data protection laws, especially incorporating specific references under the Sections 65 - 72A of the IT Act, 2000"

Annexure 'A' - Relevant Sections in ITA 2000

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	If a person denies access to an authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
72A	Punishment for disclosure of information in breach of lawful contract	Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person	Imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both

9th Floor, Haryana Civil Secretariat, Chandigarhनौवींमंजिल, हरियाणासिविलसचिवालय, चण्डीगढ़
Tel./दूरभाष:Secretary/सचिव: 0172-2704922, Fax, QSDI:0172-2705529
E-mail/ई–मेलmdhartron-hry@gov.in Website/वैबसाइट:www.haryanait.gov.in