Deloitte.

Cyber crimes Act
Top 10 Do's and Don'ts

	Cyber incident response and digital forensics	Cyber security (protect and defend your organisation against cyber crime)	Third-party software management	Data management practice
DON'T…	…attempt to self-investigate the incident. Unless your organisation has an in-house team or external service provider that is qualified and experienced with managing a cyber incident. Failure to do so, while not following established best practice guidelines and associated methodologies in accordance with the Act may, at the very least, result in the destruction of evidence and is likely to render evidence inadmissible in a court of law – thus hampering attempts to successfully prosecute.	…design security controls as a separate activity to system design. Cyber criminals exploit vulnerabilities introduced to a business caused by insecure design.	…process company information using suspicious third-party applications/software. Choose third-party applications wisely. Avoid suspicious applications and rather use applications developed by vendors that you trust. Always limit the amount of information third-party applications can access.	…read the Cyber crimes Act in isolation – other pieces of legislation such as POPIA, various regulatory codes (e.g., banking industry etc.) also deal with the subject. It is critical for companies to ensure that policies factor in all applicable legislation such as POPIA, regulatory codes etc. as well as common sense and best practises.
DO…	…use an experienced and qualified team to investigate cyber incidents. …use qualified and experienced Digital Forensic experts to identify and preserve electronic evidence. …establish a process to deal with law enforcement and investigator requests and orders.	…ensure appropriate logical and physical access control and application of least privilege principle is applied to all business areas, and embed security principles as part of business processes such as change management and adopt and promote security as a business enabler.	…ensure your organisation is aware of approved software allowed to process client and company information. This includes approved data storage solutions. …security test third-party software modules before use and monitor during use.	…adopt and adapt data management standards for cyber. Establish a continually updated "catalogue" of data sources and the content of each one, with standards for formatting, naming and combining. Catalogue data sources for business applications, email systems and data centre platforms. And extend the exercise to security analytics. …adopt unique data storage requirements. The source data must be stored together in a manageable way. It's not just storing large volumes of content, but also anticipating how you will use the data and what detail to store for how long. Enough history is required for analysts to establish baselines and do retrospective investigations. …collect only the most important information. Your data's external value will be reduced. Data security is improved by lowering the external value of your data since hackers are less likely to take low-value data and align to the POPIA requirements for data minimisation.