Create a hardware, software and information systems inventory.

Determine how the loss or short-term unavailability of data might impact operations.

Update and test data backup, recovery and contingency procedures.

Ensure that password access on computers coincides with the level of actual access needed by any given employee based upon job description.

Establish detailed password guidelines, specifying password length and acceptable configuration and requiring periodic password changes and other protection protocol.

Reposition computer monitors and apply automatic log-out mechanisms to assure systems security.

Install virus-scanning software on all relevant devices on and offsite.

Conduct phishing campaigns to test the susceptibility of personnel to click on suspicious links that can result in system infiltration.

Create forms to document investigation, mitigation, and resolution of security incidents.

Provide formal risk assessment and cybersecurity training and alert personnel that they are subject to administrative monitoring, thus eliminating any expectation of privacy.

Execute agreements contemplating vendor and third-party security breaches.

Provide detailed instructions regarding the reporting and documentation of security breaches, including to whom such breaches should be reported—governmental authorities or otherwise.

Produce an audit log of excessive or unusual systems activity.

Require that all lost or stolen access devices such as cards and keys, company laptops or mobile devices be reported.