Compliance checklist

The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)

The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

Explanation: N/A

General Data Protection Regulation (GDPR) __X__

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation: With such a low level of security in place at Botium Toys, they are currently not adhering to GDPR regulations. Customer PII and SPII are being handled worldwide and if the customers data is breached, they need to be made aware of the incident as soon as possible

Payment Card Industry Data Security Standard (PCI DSS) __X__

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation: Customer SPII which is stored by the company for transactions and processes are not secure so PCI DSS standards need to be put in place and it made sure that the company are fully compliant with regulations

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a federal law established in 1996 to protect U.S. patients' health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

Explanation:

System and Organizations Controls (SOC type 1, SOC type 2) __X__

The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Explanation: Low level security on customer and employee technical assets means SOC type 1 & 2 regulation must be adhered to and company standards must meet the criteria to enforce appropriate user access for internal and external (third-party vendor) personnel