

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: Botium does not need to adhere to FERC-NERC regulations as it has no connection/ conducts no business in relation to electricity or the US/North American power grid

☒ **General Data Protection Regulation (GDPR)**

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: Botium needs to adhere to GDPR regulations as it conducts business with customers in the E.U. and also will store SPII & PII of people who reside in the E.U.

☒ **Payment Card Industry Data Security Standard (PCI DSS)**

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: Botium will need to adhere to the PCI DSS regulations and standards as a large majority of Botiums business is conducted online, this means a large portion of their transactions will be conducted with credit cards and customers personal information will be used and stored as a result of this.

☐ **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: Botium does not take, use or store customers' health information therefore does not need to adhere to HIPAA regulations.

☒ **System and Organizations Controls (SOC type 1, SOC type 2)**

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: Botium will needs to establish appropriate user access for both internal and external personnel to ensure the integrity and safety of data and to mitigate risk