What is the Utah Cybersecurity Affirmative Defense Act (UCADA)?

The Law seeks to incentivize individuals, corporations and entities to maintain reasonable safeguards for protecting personal information by providing an affirmative defense in litigation flowing from a data breach. If a person or organization creates, maintains, and reasonably complies with a well written cybersecurity program that is in place at the time of the breach, they will be able to take advantage of an affirmative defense to certain claims.

REQUIREMENTS

Written cybersecurity programs must satisfy several requirements to warrant the act's protection:

Technical

Administrative

Physical

Safeguards must be designed to:

- Protect security, confidentiality, and integrity of personal data
- Protect against any anticipated threat or hazard to the security, confidentiality, or integrity of personal data.
- Protect against a breach of system security.
- Reasonably conform to a recognized cybersecurity framework.
- Be an appropriate scale and scope for a variety of factors including:
  - **Size of the organization**
  - **Business nature and services**
  - **Sensitivity of the information protected**

WIN FOR UTAH COMPANIES:

The affirmative defense model established by Utah, Ohio and Connecticut is a win for companies and consumers. It incentivizes best cybersecurity practices and protection of personal data, while providing a safety net for companies who face litigation due to a data breach.

WAYS TO BE COMPLIANT WITH UCADA

Protect Data - Off-site & offline data backups: 3 copies of data + 2 different media + 1 backup copy off-site

Test Security - Utilize penetration tests to test the security and resiliency of your network

Update Software - With the latest security patches

Create a Well-Written Cybersecurity Program - That describes how data will be protected and how data will be restored if needed

Train Employees - To be aware of ransomware and phishing tactics

Perpetual Storage is the Solution

Safe. Secure. Reassu

We are an underground company (literally) that most people have never heard of. This gives us an edge by keeping us under the radar of potential attackers. We provide a safe, more secure backup solution compared to Big Tech who say cloud storage is the future and the only secure way to back up data. They're wrong. Isolated Data Tier is the next iteration of the cloud that combines the convenience of the cloud with the security of offline, air-gapped measures.

We are the solution that ransomware attackers don't want CEO's to know about.

We do things differently. We build safer, better, rock solid offline data backup solutions into a granite mountain. We safeguard your company from cybersecurity threats and bad actors that want nothing more than to rob you and your organization of financial resources, credibility, and hijack your peace of mind and sense of security.

UCADA & PSI

FEATURES/PROTECTIONS	BIG TECH CLOUD SERVICES	ISOLATED DATA TIER
Provides Protection from Natural Disasters	✔*	✔
Requires Encryption	✔*	✔
Provides a Fully Managed Infrastructure	✔*	✔
Provides Off-Site BackUp	✔	✔
Provides Protection from Employee Negligence		✔
Protects Against Ransomware		✔
Provides Protection from Corrupted Data		✔
Provides Protection from Insider Theft		✔
Provides Offline- Airgap Service		✔

*Sometimes