The MPAA (Motion Picture Association of America) and CDSA (Content Delivery & Security Association) have established the Trusted Partner Network (TPN) as a global, industry-wide film and television content protection initiative to help media organizations prevent leaks, breaches, and hacks.

As an established storage solution in the media space, SwiftStack clients are often tasked with responding to TPN/CDSA/MPAA audit questionnaires and providing security-relevant information about their SwiftStack deployment(s).

SwiftStack is used in production at massive scale by some of the biggest and most security-minded media organizations in the world. SwiftStack provides all of the features and capabilities necessary to design and maintain systems and workflows that are in accordance with the MPAA's, CDSA's, and TPN's best practices.

The intention of this document/page is to answer common content-security related questions and assist SwiftStack media clients as they respond to security questionnaires and work through audit processes. Please keep in mind that as a software-only private cloud storage platform, SwiftStack is typically relevant to only a limited subset of items on these questionnaires.

The following best practices and responses are based on the MPAA's Application & Cloud Guidelines, specifically the **Data Security** section under *Cloud Security*.

Regarding the "Provider Overview" on page 5, SwiftStack typically falls under the "Private Cloud" category/service, but may also be employed as "Hybrid Cloud" and IaaS (Infrastructure as a Service) depending on the client and use-case.

Best Practice: Implement a process to provide all relevant logs requested for good cause to clients in a format that can be easily exported from the platform for analysis in the event of a security incident.

SwiftStack Implementation: The SwiftStack Controller provides the ability to quickly and easily configure the cluster to send logs to a central logging repository via syslog. SwiftStack clients often parse and retain these logs for sharing and analysis via technologies like Splunk and ELK.

Best Practice: Consider providing the capability to use system geographic location as an additional authentication factor.

SwiftStack Implementation: While this is not a default configuration option, the SwiftStack platform supports custom middleware that could be written to support this kind of geo-restriction functionality. SwiftStack clients often implement this kind of functionality via edge firewalls.

Best Practice: Provide the capability to control the physical location/geography of storage of a client's content/data, if requested.

SwiftStack Implementation: SwiftStack supports this in core functionality via Storage Policies, which can be configured to control and restrict the physical placement of stored data.

Best Practice: Establish procedures to ensure that non-production data must not be replicated to production environments.

SwiftStack Implementation: As a general purpose storage endpoint, SwiftStack provides the ability for administrators to restrict where data is located, both physically and logically. SwiftStack clients typically meet this requirement via a combination of separate storage accounts and containers, storage policies, and network ACLs.

Best Practice: Establish, document and implement a published procedure for exiting the service arrangement with a client, including assurance to sanitize all computing systems of client content/data once the client contract has terminated.

SwiftStack Implementation: While establishing, documenting, and implementing such a procedure falls to the client, SwiftStack's logging and control mechanisms make this an easy process for storage administrators.

Best Practice: Establish and document policies and procedures for secure disposal of equipment, categorized by asset type, used outside the organization's premises.

SwiftStack Implementation: SwiftStack is a software-only solution and therefore separate from any policies and procedures related to hardware or equipment. However, SwiftStack's (optional) encryption at rest will maintain data security regardless of the disposal method of the underlying physical assets.

Best Practice: Implement a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference.

SwiftStack Implementation: SwiftStack synchronizes time via NTP by default.

Best Practice: Design and configure network and virtual environments to restrict and monitor traffic between trusted and untrusted connections.

SwiftStack Implementation: SwiftStack is a software-only solution and therefore separate from configurations related to network hardware and virtual environments.

Best Practice: Design, develop and deploy multi-tenant applications, systems, and components such that client content and data is appropriately segmented.

SwiftStack Implementation: SwiftStack is multi-tenant by design and can be configured to segment data in any fashion desired by the client's storage administrator(s).

Best Practice: Use secure and encrypted communication channels when migrating physical servers, applications, and content data to/from virtual servers.

SwiftStack Implementation: SwiftStack facilitates encryption for data in transit as well as at-rest. Encryption in transit is provided via SSL/HTTPS and encryption at-rest via AES-256 encoding. See SwiftStack's Technical Brief on Encryption for more info!

Best Practice: Implement technical measures and apply defense-in-depth techniques (e.g., deep-packet analysis, traffic throttling, black-holing) for detection and timely response to network-based attacks associated with unusual ingress/egress traffic patterns (e.g., NAC spoofing and ARP poisoning attacks and/or DDOS attacks).

SwiftStack Implementation: As a software-only storage solution, defense-in-depth techniques described above are typically conducted at technology layers above SwiftStack. However, SwiftStack has written custom middleware to help mitigate the impact of brute force attacks and leaked credentials; and similar techniques could be applied to assist with other mitigations at the storage layer if desired by the client.

Best Practice: Establish and document controls to secure virtualized environments.

SwiftStack Implementation: SwiftStack is a software-only solution and therefore separate from configurations related to network hardware and virtual environments.