Security Awareness Training – Key Notes

Awareness - Your Role

YOU are the first line of defense against security attacks! Help reduce the risk to Synamedia.

At Synamedia, we're all about keeping our IP (Intellectual Property) and customer data secure. To ensure that we are all aware of the threats we face daily, all employees undergo yearly (mandatory) security awareness training.

Phishing Mail

SYNAMEDIA receives ~20,000 Phishing mails monthly, and most of them are blocked by our Microsoft Advanced Threat Protection (ATP).
Phishing is a method of trying to gather sensitive information from employees using deceptive e-mails and websites. Variations include SMS text messages, social media connections, and phone calls.
When you suspect a phishing email:

- Check where it came from – are you familiar with the sender or the email address?
- Stop, look, and think - before you click the link or open an attachment!
- Do you see anything strange or out of the ordinary about the email? If you do, call the sender and verify that they sent it to you.
- "When in doubt, throw it out." Report the phishing message using Outlook Report button, or simply delete.

> **IMPORTANT!**
>
> The change in our work habits due to COVID is also a change in the risks to Synamedia content. To help mitigate these risks, we wrote a guideline for working from home. The document contains answers to questions about topics such as networking, data protection, physical measures, and much more.

Password Policy and End-User Protection

1. All Synamedia passwords must be unique. They must contain:
   a. At least 10 (ten) alphanumeric characters and a maximum of 64 characters
   b. Both uppercase and lowercase letters
   c. At least one number (for example: 0-9)
   d. At least one special character (for example: $%^&*() _+|~-=\`{}[]:";'<>?,/)
2. Passwords must not be reused. (Technically, you can reuse a password after 10 new ones, but Synamedia doesn't recommend it.)
3. Do not use your Synamedia password for any other authentication/login.
4. Use your Synamedia account ID and email for business purposes only.
5. Ensure all passwords are:
   a. Stored securely (e.g., though a validated password vault mechanism)
   b. Not written down
   c. Not kept anywhere at home or in the office (unless secured, see a.)
   d. Not shared with anyone, including co-workers, managers and IT helpdesk
   e. Changed every 6 months
6. All accounts must utilize Multi Factor Authentication (MFA) where possible.
7. All users are a part of the IT-enforced Microsoft Conditional Access; this policy allows only managed devices to access Synamedia corporate resources.
8. All devices synchronizing Synamedia mail must be managed by Synamedia internal mobile device management (such as Intune or JAMF).

Clean Desk Policy

1. Keep your desk clean, without papers and devices that can be stolen.
2. Lock up devices and documents that may include Intellectual Property (IP), both in the office and at home.
3. Dispose of waste correctly using shredders and secure disposal.
4. Correctly dispose of unused hard drives and SD cards according to the Data Media Sanitization Guidelines.

Protect Your Device

1. Any device at Synamedia must have an owner.
2. Any device must have updated OS, latest (most recent and IT-approved versions) patches and updated anti-virus installed.

3. Always keep your devices and IP with you when these are not secured in the office or at home.
4. Do not take classified (Secret or Highly Confidential) documents out of Synamedia-protected environments.
5. Physical Security: Report suspicious incidents and lost items to the (24x7) Security Operations Center (SOC) at: soc@synamedia.com
6. Do NOT leave your Synamedia-provided laptop in your car, *(*not even in the trunk or under the seat*).*
7. Avoid using USB flash drives. If you must use one for business reasons, contact IT for instructions and only use a USB device that is provided by Synamedia or fresh out of the shop.
8. Prevent *shoulder* surfing in public areas, on public transport, etc, by avoiding work where others can examine your screen from behind your back. A privacy filter can be installed on the screen to reduce the risk.
9. Do not plug your device into a PUBLIC USB charging point. Always use an AC connected charger.

Wi-Fi

1. Use a VPN or cell phone access point connected to a Cellular network (Tethering).
2. Try to avoid using free public Wi-Fi. If you must connect to the public Wi-Fi, always use the Synamedia VPN.

Data Security

Data Protection

> **NOTE**
>
> All staff must be extremely careful to follow data protection requirements at all times, both in and out of the office. These requirements appear in other standards, but we are repeating them here to emphasize their importance.

1. Staff shall not copy Synamedia data on personal devices or unapproved Cloud services.
2. Staff shall use Synamedia assets (for example, laptop/USB etc.) for Synamedia business purposes only.
3. Staff shall ensure that laptop data is backed up on IT-approved storage repositories.
4. Staff are encouraged to use password managers (for example, Keeper, LastPass, BitWarden etc.) and refrain from writing down passwords.

5. Staff shall store business-related printed documents in a secure, locked location when not in use.
6. Staff shall shred documents that are no longer in use as soon as possible using local Synamedia office cross-cut shredders.
7. Staff shall use the company-provided dedicated USB drives for Synamedia business requirements.
8. Staff shall avoid charging company assets (laptops/mobile phones) using unknown/untrusted public charging stations.
9. Staff shall never take secret material outside of Synamedia premises. If there is a business need, approval from VP and InfoSec must be obtained.
10. Staff shall use PGP for any secret mail communication.

Data Classification

All Synamedia documents must be classified.

The business owner is responsible for correctly defining the data classification, using the table below as a guide.

Public	*All included information has no significance to areas such as internal technologies, how we conduct business or opportunities-in-progress, internal procedures, or policies.* ■ Non-sensitive or generic solution documents, marketing materials that are cleared for open outside distribution to customers, vendors, journalists, publishers, and others. ■ For example, marketing product descriptions, generic product operations guides.
Confidential	*Exposure of some included information may result in damage to the company.* ■ Internal references or information ■ Information released to vendors or customers only with non-disclosure agreements. ■ Any information limited to a specific customer or specific project.
Highly Confidential	*Leaking this information* ***could result in severe damage but can be mitigated with a disaster recovery plan*****.** ■ Included information has major significance in areas such as internal core technologies, conducted business or opportunities, or internal procedures or policies. ■ For example, security designs, major business plans, contracts with third parties, employee private information and customer secret information.

Secret	*Leaking this information* ***could cause irreversible damage to the company.*** ■ All information classified 'Secret' may only be exposed to intended persons on a "need to know" basis. ■ For example, conditional access secrets, security chip architecture, and internal algorithms. Secret content must be kept securely in storage that is not connected to the public internet, extranet, or enterprise intranet.

Where Should You Store Your Data

1. **Document Management System (DMS)** - This is the ONLY place within Synamedia to store documents, and this replaces all previous document locations.
2. **Teams** -Teams groups can be created by anyone and are generally used for small teams of people for preliminary collaboration on intellectual property files that are stored in DMS, or to store team-specific documents which do not need to be retained long-term.
3. **OneDrive -** OneDrive is your own work-related personal hard drive in the cloud. It is not a place for knowledge/documents/data that need to be shared in the long term, which must be stored in DMS. OneDrive can be accessed from File Explorer on your laptop and from a browser.
4. **Confluence -** Confluence is a wiki that is designed as a simple collaborative platform to manage knowledge systems. The idea is to improve a team's efficiency, as they can easily collaborate in one place, with version control and collaborative editing.

   We use Confluence to hold technical engineering information, including customer information. Our Confluence wikis foster knowledge-sharing across the organization. If you want to share documents using Confluence, copy a link to the DMS document to the Confluence page. Avoid uploading of documents.

Cloud Security

Standard Cloud Security Requirements

1. Personal cloud service accounts shall not be used for business purposes.
2. Users that need to store, process, share and manage data in a cloud environment shall use only approved cloud services.
3. All passwords configured in the cloud service shall comply with the Synamedia Password Policy and Password Construction Standard.
4. To use third-party cloud service providers (CSP) for Synamedia operations, the Synamedia sponsors of a CSP must complete a review (Synamedia Cloud Services Engagement process) of the CSP before it can be used for Synamedia business.

Cloud Security Requirements for Cloud Admins

1. Make root and Admin passwords complex with MFA enabled
2. Utilize Synamedia SSO (Single Sign On) instead of local IAM (Identity Access Management) cloud users.
3. Enable MFA on all IAM cloud users.
4. Delete any unused IAM cloud users.
5. Rotate all Access Keys periodically.
6. Limit the admin permissions of IAM Cloud users and roles.
7. Review all security groups and NACLs (Network Access Control Lists).

> **CAUTION!**
>
> Traffic from 0.0.0.0/0 is not allowed unless necessary and only on specific ports.

8. Ensure AWS S3, GCP Cloud Storage and similar services in other cloud providers are not public and public lock is enabled.

Contact InfoSec if you:

- Suspect Synamedia confidential info has been compromised.
- Suspect a computer or network has been hacked.
- Are designing a new way to provide employees, partners, or customers with access to internal and propriety information.
- Would like general advice about security.

Infosec Policies, Guidelines and Standards

All documents are stored in our DMS.

Policies

Acceptable Use Policy	All employees, contractors, consultants, temporary, and other workers at Synamedia and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the Synamedia Code of Business Conduct, Synamedia policies and standards, and local laws and regulation.

Access Management Policy	This policy establishes requirements for managing user and administrative access to data and infrastructure (devices, applications, and services) by establishing proper controls for authentication, authorization, and auditing. Synamedia recognizes three types of accounts used for this purpose: ■ User accounts – personal and non-transferrable ■ Shared accounts – used for emergencies only though an offline procedure. ■ Generic accounts – non-personal account used for batch processing or repeating tasks with one owner.
Audit Policy	The policy establishes the authority for members of Information Security (InfoSec) to conduct a security audit at Synamedia. An audit may be conducted to: ■ Ensure confidentiality, integrity, and availability of information and resources ■ Investigate possible security incidents ■ Ensure conformance to Synamedia security policies ■ Assess user or system activity where appropriate.
Cloud Security Policy	This policy specifies the general-to-all-cloud-services requirements to evaluate, secure, and authorize all cloud services where Synamedia consumes a third-party service or where it functions as a cloud service provider to host or offer cloud services for customers, partners, or employees.
Content Security Policy	This policy establishes content protection requirements and roles and responsibilities for securing and protecting content throughout its lifecycle, from collection or creation to processing, storage, use, and destruction.
DMZ Policy	This policy establishes the Synamedia policy for the design, maintenance, and use of DMZ environments.
High Value Endpoint Protection Policy	Synamedia's InfoSec team has identified endpoints that store sensitive information such as security specs, business & financial plans, and identifiable personal information. If these endpoints are attacked, breached or obtained by a third party, there is a potential for severe damage to Synamedia's business.
Incident Management Policy	This policy applies to any real or suspected event, whether technical, physical, organizational, or otherwise, that may adversely affect the security of data or the systems that process, store, or transmit that data.
Information Security Exception Policy	This defines the policy for requesting an exception to a published Information Security (InfoSec) policy or standard, in order not to be in compliance with that policy or standard
Intellectual Asset Policy	Synamedia intellectual assets provide the technological advantage and market differentiator for Synamedia and its customers' continued success. Protecting intellectual assets is a top priority and the responsibility of everyone to ensure that Synamedia is at the forefront of the competitive landscape.
Lab Security Policy	This policy outlines how Synamedia will protect its lab environments and apply controls such as access control, device hardening, vulnerability management, network segmentation, and password protection

Password Policy	This policy establishes the standard for the creation, protection, and frequency of change for strong authentication credentials.
Software Usage Policy	The purpose of this policy is to outline the rules for the installation of software on Synamedia owned & managed computing devices.

Guidelines

Extranet Network Connection Guidelines	This document provides a summary of extranet partner network connection requirements for “connected to Synamedia” partner sites.
Extranet Partner Guideline	This policy applies to the use by an approved external partner of information, electronic and computing devices, and network resources to conduct Synamedia business or interact with internal networks and business systems, whether owned or leased by Synamedia, the employee, or a third party.
Information Security Exception Guideline	This document describes the process for obtaining an exception to a published Information Security (InfoSec) policy or standard, in order not to be in compliance with that policy or standard
Network Access Guideline	This policy applies to all electronic and computing devices, whether owned or leased by Synamedia, an employee, or a third party, that connect to the network or provide wired, wireless, or remote access to the network.
Service Security Guidelines	These guidelines specify the security requirements which software, tools and applications must satisfy when being used or implemented within Synamedia infrastructure and Synamedia owned Cloud platforms.
Supplier Security Guidelines	These guidelines specify the minimum-security requirements to be followed by the suppliers and service providers. These guidelines assist Synamedia employees when reviewing a new supplier and service provider to ensure they follow these Synamedia supplier security guidelines
Working from Home Standard and Guideline	This document establishes information security standard and guidelines for Synamedia employees working from home.

Standards

Internet Firewall Standard	This standard specifies the infrastructure requirements that firewalls must satisfy to control both ingress and egress traffic as well as traffic moving between security zones on Synamedia networks.
LAN Security Standard	This document provides standards for Phase 1 of building and maintaining the Synamedia local area networks (LAN) in all Synamedia locations.
Password Construction Standard	This standard specifies the requirements for creating a strong password, passphrase, or personal identification number (PIN).

Physical & Environmental Security Standard	This document establishes the Synamedia standards for preventing unauthorized physical access, compromise, theft, or damage to business premises and information processing facilities.
Security Logging Standard	This document establishes infrastructure logging standards on Synamedia systems to support both regulatory compliance and the logging, event monitoring and incident handling requirements for Synamedia.
Trusted Device Standard	This standard specifies the requirements that user devices (company or otherwise supplied devices, e.g., laptops, mobile phones, etc.) must satisfy to be trusted on the Synamedia corporate network.
Vulnerability Management Standard	This standard establishes requirements for vulnerability management across the various business units
Wireless Communication Standard	This standard establishes the requirements for wireless devices to access a Synamedia network and infrastructure devices that provide access to the network.