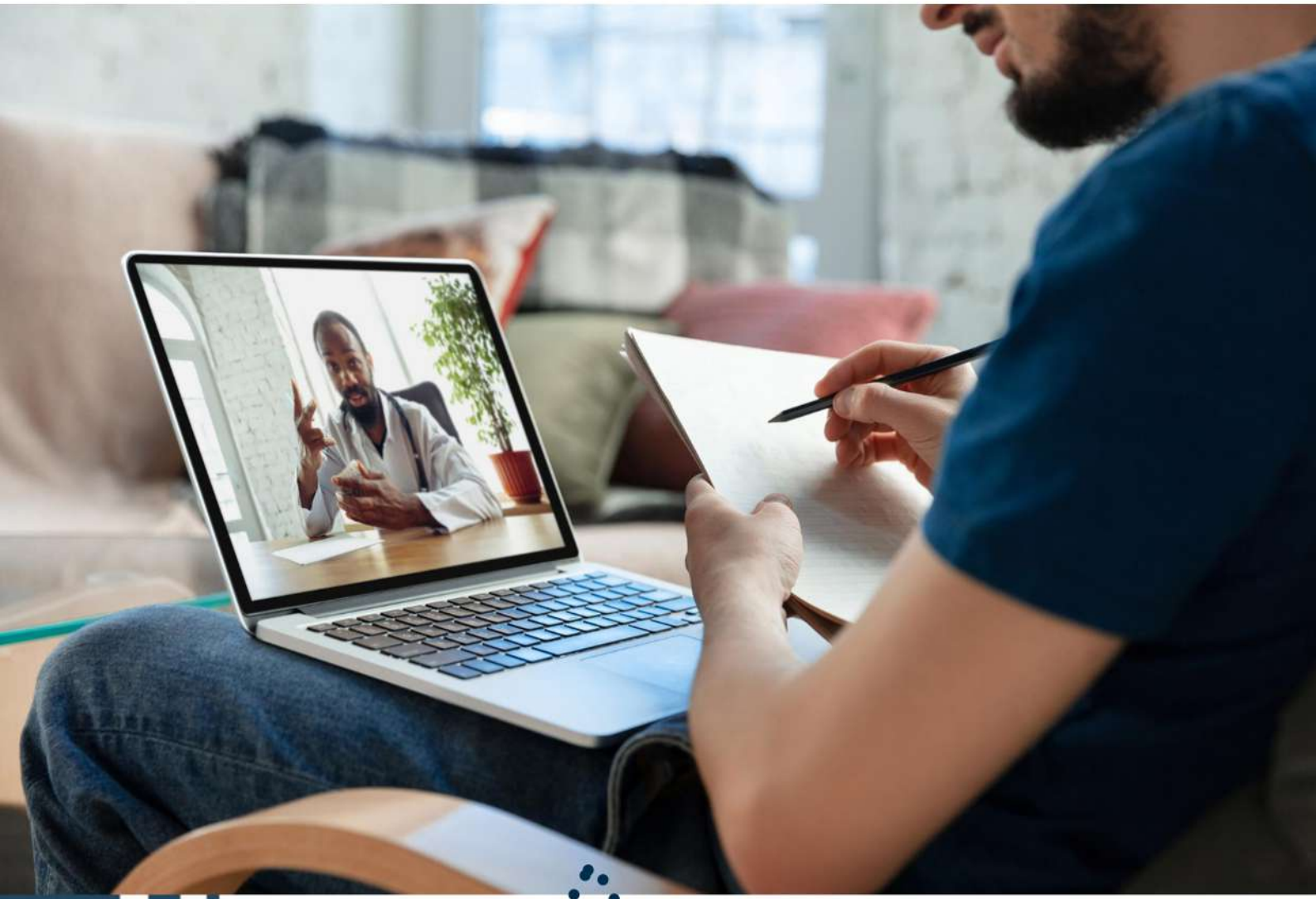
Zetlan Technologies

CyberSAFE

ZETLAN TECHNOLOGIES
www.zetlantech.com

Online Course



Course Modules

Compliance

1.Identify organizational security compliance requirements.

- Types of organizational compliance requirements
  - Password policy
  - Internet usage policy
  - Data protection
  - Personally Identifiable Information (PII)
  - Personal Health Information (PHI)
  - Acceptable Use Policy (AUP)
- On site vs. remote
- Equipment
- Shared resources (passwords, mailboxes, etc.)
- Job function differentiation
  - Facility policies
- Employee/visitor access
- Badge requirements
- Key policies
  - Ramifications of non-compliance

2.Identify legal compliance requirements.

- Types of legal compliance requirements
  - Regulation/law
- HIPAA
- SOX
- GDPR
- NISD
- e-privacy directive
  - Legal consequences of non-compliance

3.Identify industry compliance requirements.

- Examples of industry compliance requirements
  - PCI DSS
  - ISO 27001
  - NIST

4.Identify security and compliance resources.

- Organizational compliance resources
  - Handbooks/websites
  - AUP documentation
- Updates
- Location/access
  - Departments
- Human Resources
- Information Technology
- Information Security
  - Incident reporting
- Legal compliance resources
  - Government websites
  - Legal departments
  - Insurance providers
- Industrial compliance resources
  - Industry associations/professional groups

Social Engineering

5.Recognize social engineering attacks.

- Attack vectors (points of entry)
  - Username/password
  - Organizational/personnel information
  - Physical access
  - End-user personal information
  - Email
  - Mobile device
- Attack goals
  - Data destruction
  - Data theft
  - Financial gain
  - Financial harm
  - Political gain
  - Reputation
  - Revenge
- High-value targets
  - C-suite
  - Accounting personnel
  - HR personnel
  - IT personnel

- Attack types
  - Phishing
- Whaling
- Spear fishing
  - Vishing
  - Smishing
  - Pharming
  - Baiting
  - Pretexting
  - Impersonation (CEO Fraud)
  - Quid pro quo
  - Tailgating/piggybacking
  - Shoulder surfing

6.Defend against social engineering attacks.

- Resources to defend
  - Organizational hardware/devices
  - Organizational data
  - Network access
  - Premises access
  - User credentials
- Mitigation techniques
  - Situational awareness
  - Badging systems/security checks
  - Door locks
  - Verification of requests
  - Proper disposal/deletion of sensitive information
  - Continual education/training
  - Communication
  - Compliance audit

Device and Data Protection

7.Maintain the physical security of devices.

- Organzatnal & personal devices contang potntially sensitive data
  - Laptops/computers
  - Mobile phones
  - Tablets
  - Removable storage
- Organizational device-security requirements
  - Limiting the devices that have access to sensitive data
  - Credentials
  - Acceptable devices for data storage
  - Disposal/deletion requirements
- Digital presence
  - Device logs
  - Temporary files
  - Browser history
  - Cached/saved credentials
  - IoT devices
  - Cloud storage

- Device physical security techniques
  - Proper storage/disposal/recycling
  - Loss/theft reporting
  - Locking unattended machines/devices
  - BYOD controls
- Remote wipe functionality
- Location detection

8. Use Secure Authentication Methods.

- Something you know
  - Passwords/PINs
    - Frequent changing
    - Complexity
    - Prohibiting reuse/sharing
    - Memorization vs. recording/documenting
    - Something you are
- Biometrics
  - Finger print
  - Facial recognition
  - Retinal/iris scan

- Something you have
  - Authentication apps
  - Key fob
  - Tokens
  - Smart cards
- Authentication best practices
  - Password managers
  - Covert entry (ensure nobody can watch you enter it)
  - Immediately change following breach/incident
  - Secure storage of passwords
  - Critical importance of protecting email passwords
  - Multi-Factor authentication use when possible
  - Complexity compared to sensitivity of data
  - Unique passwords for all sites and systems
  - Avoiding using easy-to-guess passwords

9. Adhere to data and sensitive data protection best practices.

- Data backups/storage locations
- Mobile device considerations
  - Information leakage through always-on app functionality
  - Accidental or intentional recording of sensitive data
    - ☒ Camera
    - ☒ Microphone

- Data security techniques
  - Alerts for access/ deletion of data
  - Data classification
  - Prohibitions against copying/printing
  - Proper disposal of printed data
  - Prohibitions against removable storage devices
  - Prohibition against mobile devices in designated locations
  - Digital presence considerations
    - Device logs
    - Temporary files
    - Browser History
    - Cached/ saved credentials
    - IoT devices
    - Cloud Storage

10. Identify potential sources of malware and prevent infection.

- Malware effects
  - System corruption
  - Spying/logging
  - Distracting/annoying
  - Device performance degradation
  - Data hijacking/ransoming
  - Data destruction
  - Blackmail
  - Advertising
- Malware types
  - Key logger
  - Ransomware
  - Adware/spyware
  - Trojan horse
  - Virus
  - Worm
  - Browser hijacker
- Malware sources
  - Trick offers
  - Rogue antivirus
  - Free software scams
  - Software piggybacking

- Confusing or obscured options (custom installations)
- Unknown/untrusted download sites
- Open Networks
- Email attachments
- Links
- Scripts in data files/software
- Advertising banners
- Infected hardware
  - Thumb drives
  - External hard drives
- Malware prevention techniques
  - Careful reading of emails/dialog boxes/offers/pop-ups/etc.
  - Malware prevention software
  - IT approval for software installation
  - Inspection of links before selecting
  - Benefit/risk analysis when installing software
  - General system behavior awareness
  - Use of only known vendors and devices
    - Verified publishers

11. Use wireless devices securely.

- Common wireless network risks
  - Eavesdropping
  - Unsecure networks
    - Private
    - Public
    - Open
  - Rogue access points
  - Evil twins
  - "Remembering" wireless networks
- Secure wireless device use techniques
  - Public network use prohibitions
  - Encryption
    - WPA2/WPA3
    - Securing Wi-Fi passwords
  - Wireless network "forgetting"
  - Evil twin avoidance
    - Misspelled network names
    - Lack of password requirements when they are expected
    - Multiple networks with similar names

Online Security and Remote Access

12. Browse the web safely.

- Well-known browsers
  - Chrome
  - Edge
  - Firefox
  - Safari
- URL construction
  - HTTP vs. HTTPS
    - Non-encryption vs. encryption
  - Top level domains
  - Domain names
  - Suspicious/spoofed URLs
    - Close spellings/misspellings
- Safe web browsing techniques
  - Current and updated web browser use
  - Deciphering web addresses
    - Shortened (Bitly)
    - Misspelled
    - Wrong top-level domain (.com v .net)
    - Redirect (changed URL)

- Unknown add-in, plug-in, toolbar avoidance
- Not clicking/tapping ads and pop-ups
- Protocol verification
- URL verification when using links
- Typing vs. clicking
- Bookmarking common sites
- Caution when using mobile devices (URLs not always visible)

13. Use email securely.

- Common email use risks
  - Frequent social engineering attacks
    - Security concern alerts
    - Requests for user credentials
    - Malware removal/IT support offers
    - Free offers
    - Monetary/inheritance scams
    - Requests for information
    - Fake invoices from debt collectors
    - Fake credit card expiry notifications
    - Urgent requests form supervisor/ executive level
- Malicious attachments
    - High-risk file types

- ZIP/ Compressed files
- .exe
- JavaScript
  - Attachment policy/regulation compliance
- Safe email use techniques
  - Imposter identification
    - Sender name vs. email address
    - Subject line topics
    - Tone/voice/grammar of sender
    - Signature lines
    - Unusual/atypical/urgency requests from seemingly valid sources
- "Bank" asking for password in email
- "IT" asking for personal info via email
  - Sender verification
    - Call back/meet in person before responding/clicking
- Email use policy compliance
- Attachment considerations
    - Approved third-party cloud storage (Dropbox, Box, etc.)
    - Password protected
  - Encrypted

14. Use social networks securely.

- Social network security considerations
  - Accidental sharing of sensitive information
  - Combined sources of data (multiple platforms, posts, replies...)
  - Disparaging/revealing comments
    - Representing yourself vs. the organization
    - Sensitive information
  - Lack of control over data and sharing
    - Confidentiality
    - Once posted, always online
    - Consent to data sharing
  - Ambiguous/lengthy confusing security settings
  - Opportunities for social engineering
  - Spoofed accounts
  - Hacked accounts
  - Strong authentication
    - Password
    - Multi-Factor Authentication (MFA)
  - Safe social networking techniques
  - Alignment with organizational social networking usage & policies
  - Thorough research and configuration of security & privacy settings
  - Caution with sharing any potentially sensitive or reputation-dmgng

- Security of credentials
- Social engineering awareness
  - Verify connections
  - Verification of content
- Fact checking

15. Use cloud services securely.

- Cloud service risks
  - Cloud service spoofing
  - Vendor changes
    - Acquisitions/mergers
    - Out of business
  - Mixing up work and private accounts (digital storage location)
  - Compromising credentials
  - Data persistence
- IoT device considerations
  - Data collection
- Safe cloud service use techniques
  - Organizational approval for all cloud-based storage
  - Local backups
  - Extra credential vigilance
    - Secure network connection

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474