



DATA SECURITY

We serve over 3,000 accounting firms across various services, and we protect each client's data through our robust information security policies that align with IRS, FTC, and AICPA standards



TABLE OF CONTENTS

This presentation provides a comprehensive overview of MYCPE ONE's data security measures, certifications, and practices designed to protect sensitive client information.

Throughout this presentation, you will learn about our:

- Industry-recognized security certifications
- Robust workplace security practices
- Comprehensive business continuity
- Planning Security training programs
- The three pillars of our data security framework

Our commitment to data security is the foundation of the trust that our clients place in us.

In This Presentation

1. Data Security Overview
2. Certifications Overview
3. SOC 2 Type I-II Certifications
4. ISO 27001:2022 Certification
5. GDPR Compliance
6. Security Practices
7. Other Security Details
8. Business Continuity Plan
9. Security Training
- 10.3 Pillars of Data Security
11. People Pillar
12. Practices Pillar
13. Processes Pillar
14. Cybersecurity Measures

DATA SECURITY FOR CPA & ACCOUNTING FIRMS

Safeguarding Practices: Comprehensive data security measures designed specifically for accounting and CPA firms to protect sensitive client information.

Client Data Protection: Ensuring confidentiality of sensitive financial information and personal data

Regulatory Compliance: Meeting industry standards and legal requirements for data handling

Security Infrastructure: Implementing robust systems to prevent unauthorized access and data breaches

Why It Matters:

- Protects client confidentiality and firm reputation
- Prevents costly data breaches and associated penalties
- Establishes trust with clients and partners
- Maintains compliance with evolving regulations

VIDEO OVERVIEW



Data Security for Accounting & CPA Firms
Safeguarding Practices | MYCPE ONE

CERTIFICATIONS

MYCPE ONE maintains industry-leading security standards through comprehensive certifications and compliance frameworks, ensuring the highest level of data protection for our clients.

AICPA SOC 2 Type I-II Certification



A voluntary Compliance Requirement for service organizations developed by the American Institute of CPAs (AICPA). It specifies how organizations should manage customer data based on Trust Services Criteria: Security, Availability, Processing, Integrity, Confidentiality, and Privacy.

ISO 27001:2022 Certification



International standard for information security management systems. The certification confirms that MYCPE ONE has implemented comprehensive security controls to protect clients' data from unauthorized access, theft, and loss.

GDPR Compliance



Compliance with EU privacy law governing personal data handling. Includes robust technical and organizational measures to safeguard data and uphold privacy rights with DPO oversight.

Security Practices



Comprehensive security measures including restricted mobile devices, paperless environment, controlled access, monitoring, and insurance coverage to ensure complete client data protection.

AICPA SOC 2 TYPE I-II CERTIFICATIONS

Certification Overview: MYCPE ONE has achieved SOC 2 Type II certification, a voluntary compliance standard for service organizations developed by the American Institute of CPAs (AICPA).

Industry Recognition: SOC 2 certification is a widely recognized industry standard. Achieving it demonstrates our compliance with various regulatory frameworks and standards such as GDPR, HIPAA, and PCI-DSS.

Trust Services Criteria:

Security: Information and systems are protected against unauthorized access

Availability: Information and systems are available for operation and use

Processing Integrity: System processing is complete, valid, accurate, timely, and authorized

Confidentiality: Information designated as confidential is protected

Privacy: Personal information is collected, used, retained, and disclosed in compliance with commitments

ISO 27001:2022 CERTIFICATION

ISO27001:2022 is the international standard for information security management systems. The certification confirms that MYCPE ONE has implemented comprehensive security controls to protect client data from unauthorized access, theft, and loss.

The ISO 27001 certification process involves a rigorous external audit by an independent certification body to ensure that our security controls meet or exceed global best practices.

The International Organization for Standardization (ISO) is a globally recognized standard-setting body that develops and publishes international standards for multiple industries and sectors.



[View Certificate](#)

GDPR COMPLIANCE

We are compliant with the General Data Protection Regulation (GDPR), a comprehensive privacy law regulating how businesses handle the personal data of EU residents. The GDPR requires businesses to implement appropriate technical and organizational measures to protect personal data and respect data subjects' privacy rights.

To comply with the GDPR, MYCPE ONE has implemented several measures, including data protection policies and procedures, employee training on data protection, regular security audits, and data breach response plans.

MYCPE ONE has also appointed a Data Protection Officer (DPO), who oversees the company's compliance with GDPR requirements.



[View Certificate](#)

SECURITY PRACTICES

MYCPE ONE has implemented comprehensive workplace measures to ensure data security and protect client information across all operational environments.



Mobile Device Policy

Mobile phones are strictly prohibited in work areas to prevent data leakage and unauthorized recording of sensitive information.



Paperless Environment

All USB ports are disabled, and the use of pens, papers, and printers is prohibited to prevent physical data extraction.



Internet Security

Internet access is continuously monitored, with personal email and social media strictly prohibited to prevent data exfiltration.



Physical Access Control

Key-card controlled access to work areas and 24x7 CCTV surveillance ensure only authorized personnel can access secure areas.



Multi-Factor Authentication

Robust authentication measures including MFA and firewall protection secure all digital systems and sensitive information.



Remote Employee Monitoring

Specialized monitoring software ensures remote employees maintain the same high security standards as on-premises staff.



Security Insurance

Comprehensive cybersecurity insurance and Errors & Omissions (E&O) insurance provide additional layers of protection.



Data Encryption

All sensitive data is encrypted at rest and in transit, ensuring information remains protected against unauthorized access.



Certified Compliance

GDPR compliant and ISO 27001 certified processes demonstrate our commitment to maintaining global security standards.

OTHER DETAILS



Zero Security Breach:
10+ year track record with no incidents



Cybersecurity Insurance Coverage:
Financial protection against cyber threats



Cybersecurity Certification:
Disaster Recovery Management expertise



E&O Insurance Coverage:
Professional liability protection



No Local Storage:
Client information never stored on local devices



IT Policies:
Comprehensive guidelines for data handling



Thorough Vetting:
Background and referral checks for all staff



General Liability Insurance:
Additional business protection layer



PCI DSS Compliance:
Secure payment processing standards

BUSINESS CONTINUITY PLAN

10% Additional Workstation & 15% Infrastructure Capacity at Anytime.

8% to 10% Staff Available on bench.

Antivirus and Malware Protected.

Computer with battery back-up (Upto 2 hours) in case of Power Outage.

Fuel Generator with back-up (Upto 2 hours) in case of Power Outage.

Cyber and Data Theft Insurance Coverage.

Insurance Cover (flood, hurricane, earthquake).

3 Dedicated Internet Lines
(1 Operational and 2 Backups).

Network Security and Firewall Protection.

BCP Response Team.

Incidence/Disaster Testing Monthly/Quarterly.

Diversified Hiring across 20+ Cities across India/Philippines.

TRAINING

Comprehensive Training Approach: At MYCPE ONE, we prioritize the security of our client data through comprehensive and ongoing cybersecurity training.

ONBOARDING TRAINING



Secure Data Handling

Teaches the principles of protecting client information, including encryption and secure data storage practices.



Password Management

Instructs on creating strong passwords, using password managers on the secured portal, and the importance of regular password changes.



Phishing Detection

Educates on identifying and responding to phishing attempts and other common cyber threats.



Safe Internet Practices

Outlines best practices for browsing the internet securely, especially when accessing client data.

ONGOING TRAINING:



Advanced Phishing Defense

Continuous training on the latest phishing techniques and defenses against them.



Software and Application Security

Updates on securing software applications that are critical to handling client data safely.



Data Transfer Policies

Training on the strict policies against copying or transferring client data without authorization, emphasizing the importance of maintaining data confidentiality.



Incident Response

Training on how to respond effectively to a data breach or security incident to minimize damage and recover data integrity.

PILLARS OF DATA SECURITY

MYCPE ONE upholds the '3 Pillars of Data Security' - People, Processes, and Practices. We ensure a trusted environment by empowering team members to safeguard client success.

Our Security Foundation:

People: A foundation of trust and expertise where every team member is empowered to protect client data

Processes: Stringent security protocols that fortify every layer of our infrastructure

Practices: Vigilant round-the-clock monitoring that upholds elevated safety standards

Our comprehensive approach to data security creates a robust framework that ensures client information remains protected at all times while maintaining operational excellence.

THE 3 PILLARS FRAMEWORK



PEOPLE

IT expertise, rigorous screening, continuous training, and strict access controls



PROCESSES

Regular audits, monitoring systems, compliance frameworks, and incident response



PRACTICES

Physical security, encryption, access management, and controlled workspaces

SECURITY OUTCOMES



Maximum Data Protection



Enhanced Client Trust



Risk Mitigation



Regulatory Compliance

PEOPLE: THE FIRST PILLAR

At MYCPE ONE, we believe in a foundation of trust and expertise. Every step we take is geared towards nurturing a secure workplace where every team member is empowered to protect our clients' data and success.

1

100-Member Dedicated & Qualified IT Team

Assign three IT specialists per 100 employees for vigilant network support and quick problem-solving, ensuring stable and secure systems.

2

Thorough Employee Screening

Conduct detailed background checks to confirm new hires' credibility and maintain organizational trust.

3

Cybersecurity Training

Regular, comprehensive training to update staff on cybersecurity awareness and best practices, arming them against emerging digital threats.

4

Role-based Access Control

Restrict data access strictly to necessary personnel, minimizing the risk of data breaches.

5

IDPS Implementation

Deploy advanced systems to detect and counteract cyber threats in real time, safeguarding network integrity.

6

Employee Confidentiality Agreement

Bind employees to secrecy through legal agreements, securing sensitive business information.

7

Employee Monitoring System

Implement screen activity tracking to bolster both productivity and cybersecurity compliance.

PRACTICES: THE SECOND PILLAR

MYCPE ONE maintains a steadfast commitment to the highest standards of data security.

Our comprehensive security measures are designed to protect against both internal and external threats, ensuring that our client's data remains safeguarded at all times.

1

Firewall Protection

We use firewalls to keep our network safe from unwanted intrusions.

2

Disabled USBs

Blocking USB ports helps us prevent data theft and stops viruses in their tracks.

3

24x7 CCTV Surveillance

Constant camera monitoring acts as our eyes, deterring and documenting any unusual activity.

4

Key Card Access

We control access to our most sensitive areas with key cards, ensuring only authorized staff get in.

5

Prohibited Mobile Devices

Personal phones and tablets are a no-go to keep our networks secure.

6

No Pens-Papers-Printers

In our work zones, we ditch paper to keep the information strictly digital and secure.

7

Restricted Internet Access

We restrict internet use to work-only websites to keep our systems safe.

8

Encryption

We keep our data scrambled and unreadable to anyone who shouldn't see it

9

Two-Factor Authentication (2FA)

We add an extra step to verify identities for safer system access.

PROCESS: THE SECOND PILLAR

Keeping our systems safe is at the heart of everything we do. We watch over our networks day and night and make sure everyone we work with meets our high safety standards.

1

Regular Security Audits

We perform systematic security evaluations to identify and address vulnerabilities, strengthening our defenses against cyber threats.

2

Data Backup and Recovery

Our comprehensive backup procedures ensure data integrity and swift recovery, protecting against data loss from various disruptions.

3

24 X 7 Traffic Monitoring

We continuously monitor network traffic to quickly identify and respond to any suspicious activities.

4

Paperless Operations

Our paperless workflows not only increase efficiency and security but also promote environmental sustainability by reducing our reliance on physical documents.

5

Incident Response Plan

A well-defined incident response plan allows us to handle security breaches effectively, minimizing damage and operational downtime.

6

Vendor Risk Management

We rigorously assess third-party vendors to ensure they meet our strict security standards, maintaining the safety of our data ecosystem.

7

Regulatory Compliance

We strictly adhere to data protection laws and regulations to prevent legal and financial repercussions and protect sensitive information.

8

No Client Data Storage

By not storing client data, we eliminate the risk of breaches, reduce potential liabilities, and enhance client trust. So we can say that there is No Downside Risk.

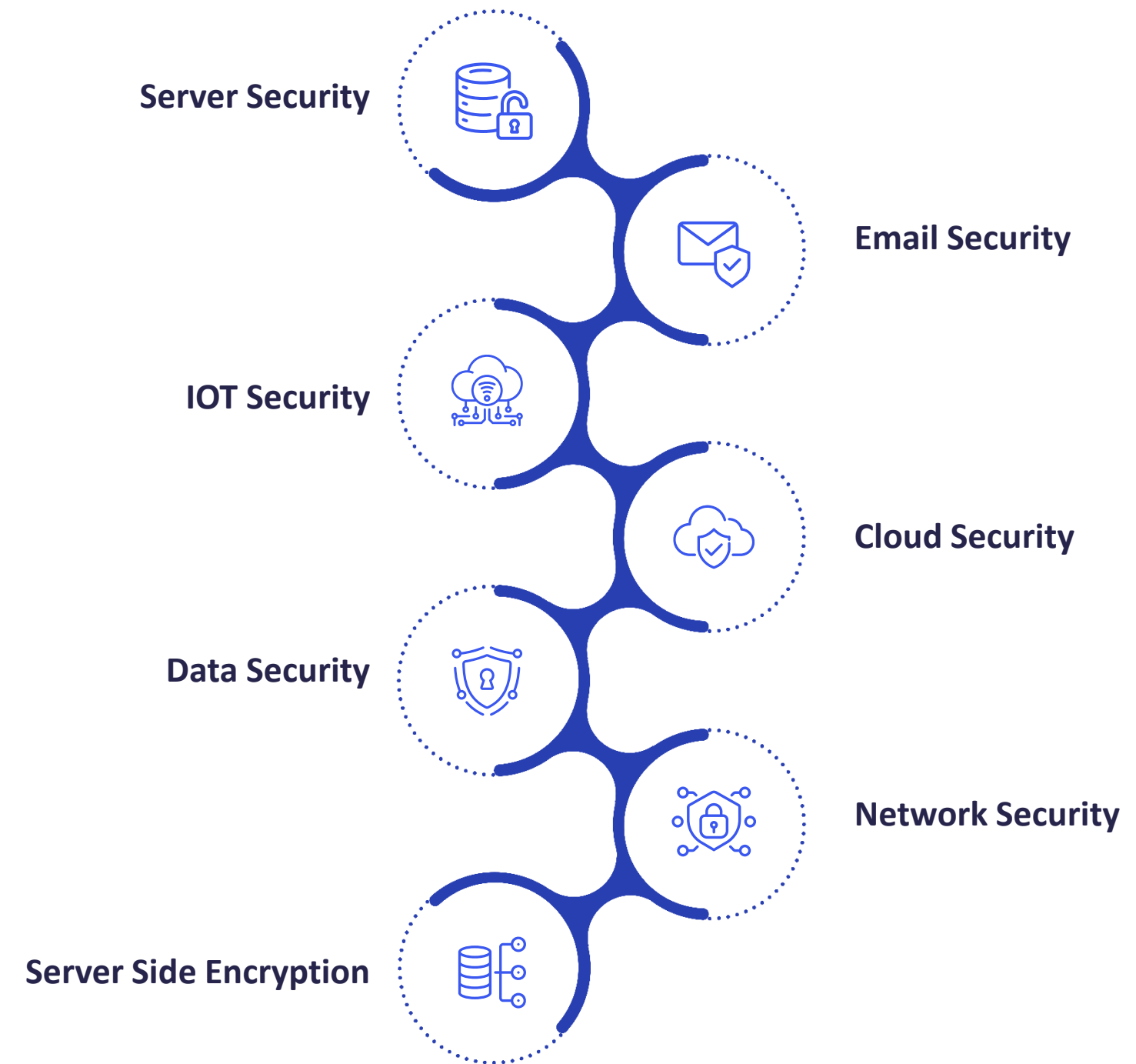
CYBERSECURITY MEASURES

In the digital age and in our line of business, protecting sensitive information is more than a necessity—it's a cornerstone of trust. Each day, we handle vast amounts of data for our clients, and the potential risks of cyber threats loom large. That's why we've committed ourselves to a rigorous cybersecurity protocol that permeates every level of our operations.

Our commitment is not just limited to technology; it includes state-of-the-art technology such as encrypted communications, secure access protocols, and continuous monitoring systems designed to detect and mitigate threats swiftly. We believe that a well-informed team is our best defense against cyber threats. Regular training sessions keep our employees up-to-date on the latest security practices and phishing threats, ensuring that vigilance is maintained through every click and every email.

This continuous education fosters an environment where security is everyone's responsibility, and caution becomes a habitual safeguard. By integrating cybersecurity into our culture, we ensure it's not just about protection—it's a promise of trust and reliability to our clients.

SECURITY ARCHITECTURE



THANK YOU!

We appreciate your attention to our comprehensive data security measures.
Your clients' data security is our top priority.

 www.my-cpe.com

 chris@mycpeone.com