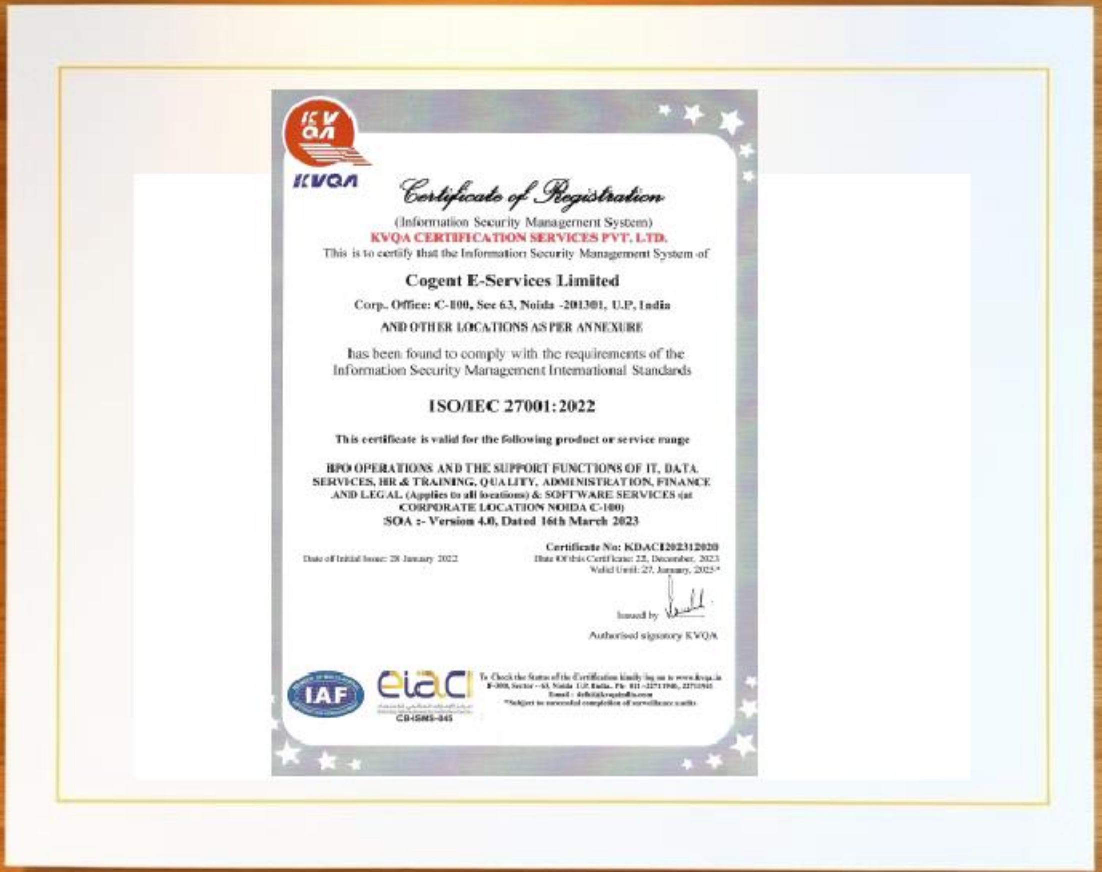
ISMS Awareness Training

Welcome to Cogent's ISMS Awareness Training. All employees, play a crucial role in protecting our company and client data.

This training will introduce you to our Information Security Management System (ISMS) and its importance in our daily operations.

○ **by Information Security Team**

Understanding ISMS 27001:2022 Certification



KVQA

Certificate of Registration

(Information Security Management System)

KVQA CERTIFICATION SERVICES PVT. LTD.

This is to certify that the Information Security Management System of

Cogent E-Services Limited

Corp. Office: C-100, Sec 63, Noida -201301, U.P, India

AND OTHER LOCATIONS AS PER ANNEXURE

has been found to comply with the requirements of the
Information Security Management International Standards

ISO/IEC 27001:2022

This certificate is valid for the following product or service range

BPO OPERATIONS AND THE SUPPORT FUNCTIONS OF IT, DATA SERVICES, HR & TRAINING, QUALITY, ADMINISTRATION, FINANCE AND LEGAL (Applies to all locations) & SOFTWARE SERVICES (at CORPORATE LOCATION NOIDA C-100)
SOA :- Version 4.0, Dated 16th March 2023

Date of Initial Issue: 28 January 2022

Certificate No: KDACI202312020
Date Of this Certificate: 22, December, 2023
Valid Until: 27, January, 2025*

Issued by

Authorised signatory KVQA

IAF

eiac

CB-ISMS-045

To Check the Status of the Certification kindly log on to www.kvqa.in
B-300, Sector - 63, Noida U.P. India. Ph: 011-22711940, 22711941
Email : delhi@kvqaindia.com
*Subject to successful completion of surveillance audits

Commitment to Excellence

Our ISMS 27001:2022 certification demonstrates our dedication to top-notch information security practices.

Employee Responsibility

As part of a certified company, you're expected to follow specific security practices in your daily work.

Continuous Improvement

This certification requires ongoing efforts to maintain and enhance our security measures.

Your Role in ISMS

1 **Understand**

Familiarize yourself with ISMS guidelines and company security policies.

2 **Implement**

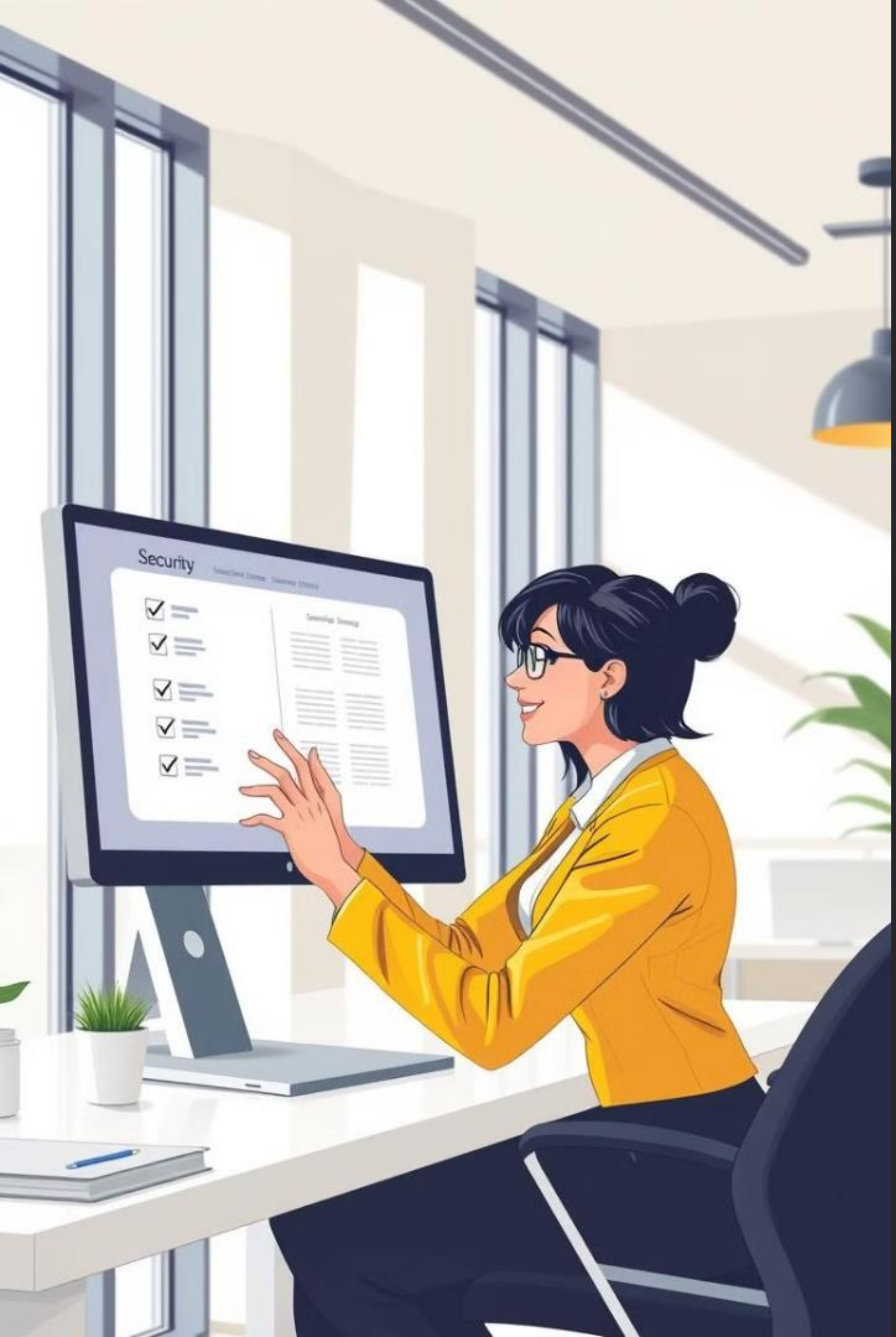
Apply security practices in your daily work, from password management to data handling.

3 **Report**

Stay vigilant and report any suspicious activities or potential security breaches.

4 **Improve**

Participate in ongoing training and contribute ideas to enhance our security measures.



ISMS Do's

Lock Your Computer

Always secure your workstation when stepping away, even for a short time.

Use Strong Passwords

Create unique, complex passwords and update them regularly to enhance security.

Report Suspicious Activities

Immediately notify your manager or infosec team about any unusual occurrences.

ISMS Don'ts

1 **Don't Share Passwords**

Keep your passwords confidential, regardless of who asks for them.

2 **Don't Leave Documents Unattended**

Secure all confidential papers, avoiding leaving them exposed on your desk.

3 **Don't Click Unknown Links**

Avoid interacting with links from suspicious or unknown email sources.

ISMS Don'ts

1 **No Mobile Phone/Storage Device/Smart watch Allowed On Floor**

Eemployees are not permitted to bring or use mobile phones, storage devices (like USB drives), or smartwatches on the operations floor.t

2 **No Tailgating**

Eemployees should not allow anyone to follow them closely through secure access points (like doors or gates) without proper authorization or access control.

3 **No Pen Paper Allowed on the floor**

Employees are not permitted to bring or use pens, pencils, or paper on the operations floor

Cogent Information Security Policy

Cogent E-Services Limited
(Hereafter referred to as “Cogent”)
INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

“Information security and its demonstration to our existing and prospective clients is critical to our survival and key to our growth.

Cogent shall use ISO 27001:2022 and its requirements as an Information Risk Management Framework to create its own Information Security Management System (ISMS).

Information security risk management will form a key component of all our processes and functions and ownership of managing risks of the assets shall rest with the asset owner.

Cogent shall implement procedures and controls at all levels to protect the Integrity, Confidentiality and Availability of information stored and processed on its systems and ensure that information is available to authorized persons as and when required.

Cogent is committed to continual improvement of its information security management system based on ISO/IEC 27001:2022 while meeting all legal, statutory and regulatory requirements.

Sd/-
ABHINAV SINGH
MANAGING DIRECTOR
27th Aug 2024. Version 2.2

Phishing Overview and Protection

1

Recognize

Learn to identify suspicious emails, links, and requests for information.

2

Verify

Always confirm the source before clicking links or providing personal information.

3

Report

Alert the IT team about potential phishing attempts immediately.

Incident Reporting

Immediate reporting of suspected incidents to the IT Security department

@ infoseccompliance@cogenteservices.com

Why Report?	How to Report	What to Include
Protects company data	Email: infoseccompliance@cogenteservices.com	Detailed description of the incident
Prevents further damage	Be prompt in reporting	Time and date of occurrence
Fulfills your responsibility	Follow up if needed	Any actions taken in response

Accessing ISMS Policies

1

Step 1: Log in

Access EMS Portal with your credentials.

2

Step 2: Navigate

Locate and click on ISMS Policy tab.

3

Step 3: Explore

Browse and review all ISMS policies.

Consequences of Non-Compliance

"If any employee does not follow these guidelines, action will be taken as per the Corrective Action Policy."

1. Verbal Warning

   Initial reminder of policy importance.

2. Written Warning

   Formal documentation of policy violation.

3. Suspension

   Temporary removal from work duties.

4. Termination

   Severance of employment in severe cases.

Thank You for Your Attention