GDPR & Information Security Policy

ONESTEP'S BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN FOR HEIS

Equivalent to BS25999 Standard

Purpose

The purpose of this Business Continuity and Disaster Recovery Plan (BCP/DRP) is to ensure that OneStep Global can continue to deliver critical services to its clients (such as Higher Education Institutions (HEIs) in the event of a disruption or disaster, and to minimise the impact of such events on our operations.

Scope

This plan covers all critical functions, processes, and resources required to support HEIs clients India operations, including personnel, facilities, technology, and data.

Business Impact Analysis (BIA)

Critical Functions

- Student recruitment and admissions support
- Partnership development and management
- Marketing and event management
- Stakeholder engagement and communication
- Financial management and reporting

Maximum Tolerable Period of Disruption (MTPD)

- Student recruitment and admissions support: 24 hours
- Partnership development and management: 48 hours
- Marketing and event management: 72 hours
- Stakeholder engagement and communication: 48 hours
- Financial management and reporting: 72 hours

Risk Assessment

Potential Threats

- Natural disasters (e.g., earthquakes, floods, severe weather)
- Pandemic or epidemic outbreaks
- Cyber-attacks or data breaches
- Power outages or telecommunication failures
- Civil unrest or terrorist incidents

Risk Mitigation Strategies

- Regular data backup and off-site storage
- Redundant power supply and communication channels
- Employee cross-training and job rotation
- Remote work capabilities and secure VPN access
- Comprehensive insurance coverage

ONESTEP'S BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN FOR HEIS

Plan Testing and Maintenance

Testing Schedule

- Conduct annual tabletop exercises and simulations
- Perform quarterly tests of specific plan components
- Evaluate test results and update the plan accordingly

Plan Maintenance

- Review and update the plan annually or upon significant changes
- Assign responsibility for plan maintenance and version control
- Communicate plan updates to all relevant stakeholders
- Provide regular training and awareness sessions for employees

Appendices

- Contact lists (internal and external)
- Vendor agreements and SLAs
- Detailed recovery procedures and checklists
- Forms and templates for incident reporting and tracking
- Training materials and awareness resources

By implementing this comprehensive Business Continuity and Disaster Recovery Plan, OneStep Global demonstrates its commitment to ensuring the continuity of critical services for HEIs clients India operations, even in the face of unforeseen disruptions or disasters. Regular testing, maintenance, and training will help to keep the plan up-to-date and effective, providing a robust framework for organisational resilience and risk management.

ONESTEP’S BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN FOR HEIS

Incident Response Plan

Incident Detection and Notification

- Establish clear criteria for declaring an incident
- Define roles and responsibilities for incident response team
- Implement an emergency communication plan (e.g., phone tree, mass notification system)

Incident Containment and Recovery

- Activate incident response team and assign tasks
- Assess the impact and severity of the incident
- Prioritize critical functions and resources for recovery
- Execute recovery procedures based on predefined strategies
- Coordinate with external stakeholders and service providers

Business Continuity Strategies

Alternate Work Arrangements

- Identify essential personnel and their roles
- Establish remote work policies and procedures
- Provide necessary equipment and tools for remote work
- Test remote work capabilities regularly

Alternate Facilities

- Identify potential alternate office locations
- Establish agreements with facility providers
- Ensure alternate facilities have adequate resources and infrastructure
- Conduct periodic tests of alternate facility activation

Disaster Recovery Strategies

Data Backup and Restoration

- Implement a comprehensive data backup plan
- Store backups in secure, off-site locations
- Regularly test data restoration procedures
- Establish data recovery time objectives (RTO) and recovery point objectives (RPO)

Technology Recovery

- Identify critical systems and applications
- Establish vendor agreements for emergency support and replacement
- Maintain an inventory of hardware and software assets
- Regularly test system failover and recovery procedures

ONESTEP’S INFORMATION SECURITY POLICY

Purpose

The purpose of this Information Security Policy is to establish a framework for protecting OneStep Global's valuable assets, including confidential data, intellectual property, and technology resources. This policy outlines the organisation's commitment to information security, compliance with relevant legislation and regulations, and the responsibilities of staff in maintaining a secure environment.

Scope

This policy applies to all employees, contractors, and third-party service providers who have access to OneStep Global's information assets, systems, and facilities.

Importance of Security

- OneStep Global recognises that information security is crucial to our success and the trust placed in us by our clients, partners, and stakeholders. We are committed to protecting the confidentiality, integrity, and availability of our information assets, as well as those entrusted to us by our clients, such as Higher Education Institutions (HEIs).
- Information security is essential to maintain our competitive advantage, comply with legal and regulatory requirements, and safeguard our reputation. We strive to create a culture of security awareness and responsibility throughout our organisation.

Legislation and Regulation

OneStep Global is committed to complying with all relevant legislation and regulations related to i

Information security and data protection, including but not limited to:

- Information Technology Act, 2000 (India)
- General Data Protection Regulation (GDPR) (European Union)
- Personal Data Protection Bill, 2019 (India) - once enacted

We continuously monitor changes in the legal and regulatory landscape and update our policies, procedures, and controls accordingly to ensure ongoing compliance.

Staff Responsibilities

All employees, contractors, and third-party service providers are responsible for safeguarding OneStep Global's information assets and maintaining the confidentiality, integrity, and availability of data.

Key responsibilities include:

- Complying with all information security policies, procedures, and guidelines
- Protecting confidential information and intellectual property from unauthorised access, use, or disclosure
- Using strong, unique passwords and maintaining their confidentiality
- Reporting any suspected security incidents, breaches, or vulnerabilities promptly
- Completing mandatory information security training and awareness programs

Managers have additional responsibilities for ensuring that their teams understand and adhere to information security policies and practices, and for fostering a culture of security awareness.

ONESTEP’S INFORMATION SECURITY POLICY

Incident and Breach Management

- OneStep Global has established an Incident Response Plan to detect, investigate, contain, and recover from information security incidents and breaches.
- All staff are required to report any suspected security incidents or breaches immediately to the designated Incident Response Team.
- The Incident Response Team will investigate the incident, assess its impact, and coordinate the appropriate response and recovery actions, including notifying affected parties and regulatory authorities as required.
- Lessons learned from incidents and breaches will be incorporated into our continuous improvement process to strengthen our security posture and prevent future occurrences.

Business Continuity

- OneStep Global maintains a comprehensive Business Continuity and Disaster Recovery Plan to ensure the continuity of critical services and the timely recovery of information assets in the event of a disruption or disaster.
- The plan is regularly tested, updated, and communicated to all relevant stakeholders to ensure its effectiveness and relevance.
- All staff are required to familiarize themselves with their roles and responsibilities under the Business Continuity and Disaster Recovery Plan and participate in periodic testing and training exercises.

Staff Training and Awareness

OneStep Global is committed to providing regular information security training and awareness programs to all employees, contractors, and third-party service providers.

Training and awareness initiatives will cover topics such as:

- Information security policies, procedures, and best practices
- Data protection and privacy regulations
- Recognising and reporting security incidents and breaches
- Secure remote work practices
- Social engineering and phishing prevention

Completion of training and awareness programs will be mandatory and tracked to ensure compliance and effectiveness.

Policy Review and Maintenance

- This Information Security Policy will be reviewed and updated annually, or more frequently as needed, to ensure its ongoing relevance and effectiveness.
- The Chief Information Security Officer (CISO) is responsible for maintaining and updating the policy, in consultation with senior management and other relevant stakeholders.
- All changes to the policy will be communicated to staff and other relevant parties in a timely manner, and appropriate training and awareness initiatives will be conducted to ensure understanding and compliance.

By implementing this comprehensive Information Security Policy, OneStep Global demonstrates its commitment to protecting valuable assets, complying with legal and regulatory requirements, and fostering a culture of security awareness and responsibility throughout the organisation. Regular training, testing, and maintenance will help to keep the policy up-to-date and effective, providing a strong foundation for safeguarding the interests of OneStep Global, its clients, and stakeholders.

ONESTEP'S INFORMATION SECURITY POLICY/GOVERNANCE STRUCTURE

Purpose

The purpose of this Information Security Policy is to establish a framework for protecting OneStep Global's information assets and ensuring the confidentiality, integrity, and availability of data. This policy outlines the governance structure, roles, and responsibilities for managing information security within the organisation.

Scope

This policy applies to all employees, contractors, delivery partners, service providers, and third-party suppliers who have access to OneStep Global's information assets, systems, and facilities.

Information Security Governance Structure

Founder/Director
The Founder/Director has overall responsibility for information security within OneStep Global. The Founder/Director ensure that appropriate resources, training, and support are provided to the information security team and that security objectives align with business goals.

Senior Information Risk Owner (SIRO)
The SIRO is a senior executive who is responsible for managing information risks across the organisation. They oversee the development and implementation of information security policies, procedures, and controls, and report to the Founder/Director on the status of information security risks.

Chief Security Officer (CSO)
The CSO is responsible for managing day-to-day protective security measures. They develop and implement security policies, monitor security incidents, conduct risk assessments, and oversee the implementation of security controls. The CSO reports to the SIRO and works closely with other members of the information security team.

Information Asset Owners (IAOs):
IAOs are responsible for managing and protecting information assets within their respective business units. They work with the CSO to identify and classify information assets, assess risks, and implement appropriate security controls. IAOs ensure that their business units comply with information security policies and procedures.

Information Risk Assessment and Risk Management Specialists
These specialists are responsible for conducting risk assessments, identifying vulnerabilities, and recommending appropriate risk mitigation strategies. They work closely with the CSO and IAOs to ensure that risk assessments are performed regularly and that risk management plans are developed and implemented.

Other Specialists
Depending on the specific needs of OneStep Global, other specialists may be included in the information security team. These could include IT security experts, compliance officers, legal advisors, or industry-specific experts.

ONESTEP'S INFORMATION SECURITY POLICY/GOVERNANCE STRUCTURE

Board-Level Oversight

- The Board of Directors is responsible for overseeing the organisation's information security compliance and auditing processes. They receive regular reports from the SIRO and CSO on the status of information security risks, incidents, and compliance.
- The Board ensures that information security objectives align with business goals and that adequate resources are allocated to support the information security program. They also review and approve information security policies and procedures.

Third-Party Security Management

- OneStep Global is committed to ensuring that its delivery partners, service providers, and third-party suppliers apply proper security controls to protect information assets.
- The CSO, in collaboration with the procurement and legal teams, is responsible for establishing security requirements for third-party contracts and agreements. These requirements should align with OneStep Global's information security policies and industry best practices.
- Third-party suppliers are required to provide evidence of their security controls, such as security certifications, audit reports, or questionnaires. The CSO and risk assessment specialists will review this evidence to ensure that third parties meet OneStep Global's security standards.
- Regular security assessments and audits will be conducted on third-party suppliers to verify their ongoing compliance with security requirements. Any identified deficiencies or non-compliance issues will be promptly addressed and escalated to the SIRO and CEO/Director if necessary.

Policy Review and Maintenance

- This Information Security Policy and Governance Structure will be reviewed and updated annually, or more frequently as needed, to ensure its ongoing relevance and effectiveness.
- The SIRO, in consultation with the CSO and other members of the information security team, is responsible for maintaining and updating the policy.
- All changes to the policy will be communicated to staff, delivery partners, service providers, and third-party suppliers in a timely manner, and appropriate training and awareness initiatives will be conducted to ensure understanding and compliance.

By implementing this Information Security Policy and Governance Structure, OneStep Global demonstrates its commitment to protecting information assets, managing risks, and ensuring the confidentiality, integrity, and availability of data. The defined roles and responsibilities, board-level oversight, and third-party security management practices provide a strong foundation for maintaining a robust information security posture and safeguarding the interests of OneStep Global, its clients, and stakeholders.

GDPR, DATA PROTECTION, COMPLIANCE, AND CONFIDENTIALITY POLICY

Purpose

Through this policy OneStep Global is committed to maintaining the highest standards of data protection, privacy, and confidentiality. This policy outlines our approach to ensuring compliance with the General Data Protection Regulation (GDPR), safeguarding personal data, and maintaining the confidentiality of sensitive information.

Scope

This policy applies to all employees, contractors, and third-party service providers who handle personal data on behalf of OneStep Global. It covers all data processing activities, including the collection, storage, transfer, and disposal of personal data.

Key Concepts

- **Personal data:** Any information relating to an identified or identifiable natural person (e.g., name, email, phone number, academic transcripts).
- **Data subject:** The people whose personal data is being processed.
- **Data controller:** The organization that determines the purposes and means of processing personal data (our company).
- **Data processor:** Any third party that processes personal data on behalf of the controller (e.g., email marketing platform).

Data Protection Principles

OneStep Global adheres to the following principles regarding personal data processing:

- **Lawfulness, fairness, and transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner.
- **Purpose limitation:** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimization:** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date.
- **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

GDPR, DATA PROTECTION, COMPLIANCE, AND CONFIDENTIALITY POLICY

Data Breach

A data breach occurs when confidential and sensitive information is stolen by an unauthorized group or individual. Data breaches are one of the end goals of many cyber-attacks.

A data breach is the unauthorized access and exposure of an organization's private information. Data breaches are often the result of a cyber-attack, and they represent an enormous security risk to both individuals and organizations.

Breached data can include proprietary company data like financial reports and trade secrets or customer info like credit cards and social security numbers. They're potentially extremely costly to companies, both financial and reputational.

There are several potential causes for a data breach:

- **Cyberattacks:** Web application attacks, social engineering, and system intrusions are the entry point for most data breaches.
- **Lost devices:** A misplaced or stolen computer or hard drive can provide a doorway for a data breach if found by the wrong person.
- **Human error:** Accidentally misconfiguration or exposing sensitive data leads to possible breaches.
- **Privilege misuse:** Insider employees–whether accidental or malicious–can cause data breaches with their ability to access sensitive information.

In the event of a data breach, OneStep Global will:

- First, stop the spread. Isolate impacted systems and lock any accounts that were compromised or used to access data.
- Second, identify the cause of the compromise. Whether it's due to faulty data storage, a successful phishing attack, or simply a lost laptop, you can't recover from a data breach until you know how it happened.
- Next, bring in all relevant stakeholders. That includes decision makers from the C-suite, security, IT, legal counsel, and PR departments. A serious data breach requires a top-to-bottom response, both internally and externally.
- You'll need to conduct a forensics investigation to further understand the cause and spread of the breach. And you'll need to alert parties impacted by the breach. Depending on your jurisdiction and the nature of the breach, there are certain regulations to follow. This is where legal counsel comes in.
- Finally, be patient. Data breaches can take several months to identify and recover from. It's not a quick process.

GDPR, DATA PROTECTION, COMPLIANCE, AND CONFIDENTIALITY POLICY

How to Prevent Data Breach Incidents: 12 Best Practices:

Strong Passwords and Authentication

- **Create strong passwords:** Complex passwords with a mix of uppercase and lowercase letters, numbers, and symbols are very important. Avoid using personal information or dictionary words.
- **Avoid password reuse:** Use unique passwords for every account. Password managers can be a helpful tool.
- **Multi-factor authentication (MFA):** MFA adds an extra layer of security by requiring a secondary verification code when logging in.

Phishing Awareness

- **Be wary of suspicious emails:** Identify phishing attempts. Common red flags include generic greetings, misspelled URLs, urgent requests, and unexpected attachments.
- **Don't click on unfamiliar links:** Hover over links before clicking to see the real destination URL. If it looks suspicious, don't click!
- **Report phishing attempts:** Report suspicious emails to the IT/ Admin department so they can be investigated and blocked.

Data Security Practices

- **Be careful what you share online:** Remember to be mindful of what information you share on social media and public forums.
- **Download wisely:** Be careful about downloading software or opening attachments from untrusted sources.
- **Data encryption:** If you handle sensitive data, explain the importance of data encryption to protect it even if it's breached.
- **Keep software updated:** Regularly update software applications and operating systems to patch security vulnerabilities.
- **Secure work devices:** Secure your laptops and desktops with passwords and to be cautious when using public Wi-Fi.

Notes

- All the new employees of OneStep Global have to go through a GDPR, Data Protection and Confidentiality training as a part of their Onboarding and Inductions at our company.
- The company reserves the right to revise, modify any or all clauses of this policy depending upon the demand of business.
- Corporate HR department will be the sole authority to interpret the content of this policy.

In case you find any issues or data breach, please reach out to the
IT Department on the below:
itdesk@onestep.global

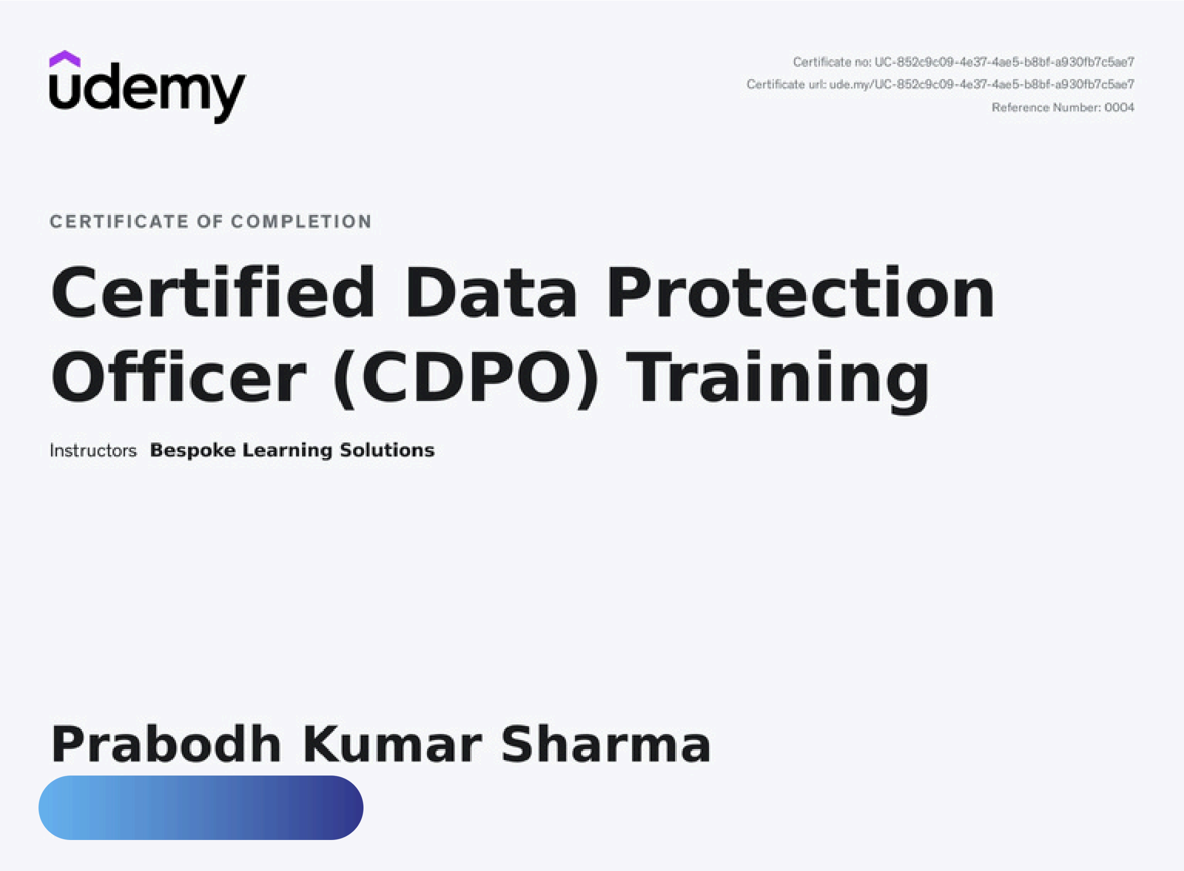
ANNEXURES

At OneStep Global, we take data protection and compliance seriously. Every employee undergoes structured training on GDPR, data protection, and compliance, ensuring that privacy and security remain at the core of our work.

All our training programs are developed under an ISO 27001-certified environment and adhere to GDPR best practices. Designed as engaging, scenario-based learning, these modules equip our teams to apply, sustain, and integrate compliance knowledge into their day-to-day work.

We also work with some of the top external LMS providers in India for compliance-based trainings, ensuring our employees have access to the highest-quality learning resources.

For reference, below are the certificates from one of our employees.



udemy

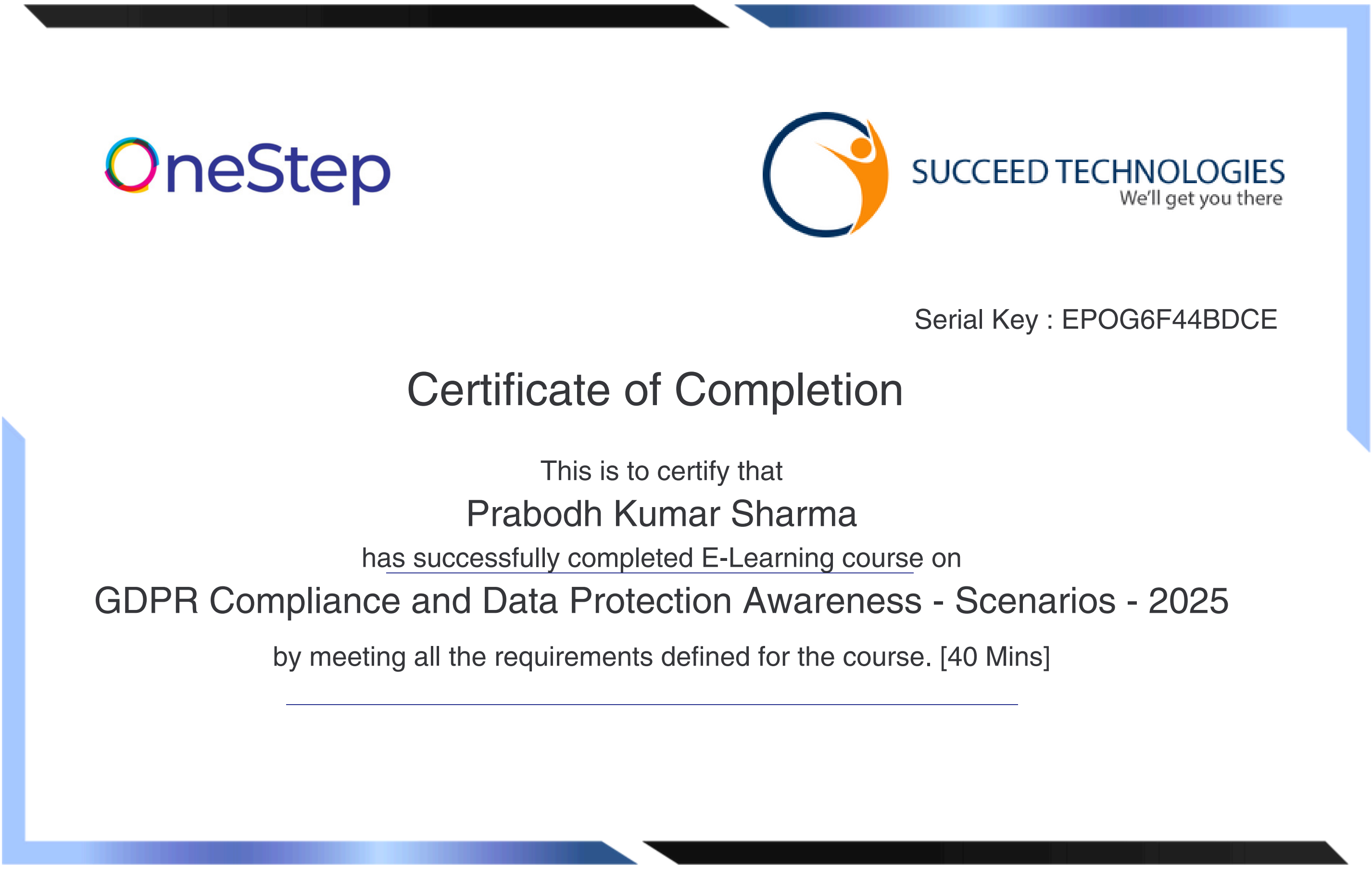
Certificate no: UC-852c9c09-4e37-4ae5-b8bf-a930fb7c5ae7
Certificate url: ude.my/UC-852c9c09-4e37-4ae5-b8bf-a930fb7c5ae7
Reference Number: 0004

CERTIFICATE OF COMPLETION

Certified Data Protection Officer (CDPO) Training

Instructors **Bespoke Learning Solutions**

Prabodh Kumar Sharma



OneStep

SUCCEED TECHNOLOGIES
We'll get you there

Serial Key : EPOG6F44BDCE

Certificate of Completion

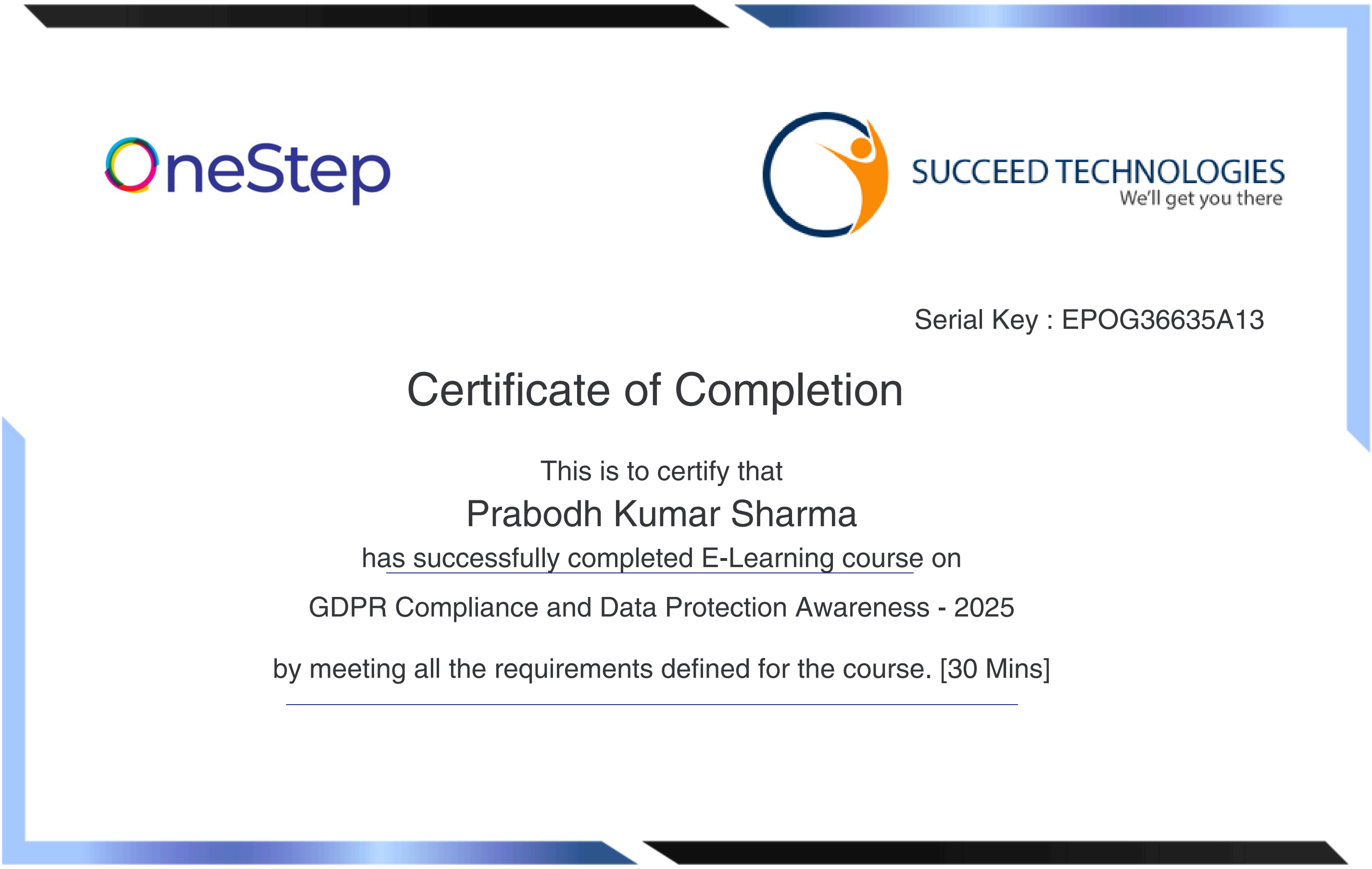
This is to certify that

Prabodh Kumar Sharma

has successfully completed E-Learning course on

GDPR Compliance and Data Protection Awareness - Scenarios - 2025

by meeting all the requirements defined for the course. [40 Mins]



OneStep

SUCCEED TECHNOLOGIES
We'll get you there

Serial Key : EPOG36635A13

Certificate of Completion

This is to certify that

Prabodh Kumar Sharma

has successfully completed E-Learning course on

GDPR Compliance and Data Protection Awareness - 2025

by meeting all the requirements defined for the course. [30 Mins]

OneStep

SUCCEED TECHNOLOGIES
We'll get you there

Serial Key : EPOGCE9D911A

Certificate of Completion

This is to certify that

Prabodh Kumar Sharma

has successfully completed E-Learning course on

Data Protection Awareness - 2025

by meeting all the requirements defined for the course. [35 Mins]