Degreed Data Privacy, Protection and Information Security Policies Overview

Degreed has comprehensive policies to ensure data privacy, protection, and information security:

- ***Data Protection Policy:***

Degreed Data Protection Policy outlines data processing principles followed by Degreed, focusing on Consumer Data and Customer data processing, applicable globally to all Degreed Staff. It includes principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, and accuracy. The policy addresses personal data breaches, sub-processing, and privacy management systems, ensuring compliance with Data Protection Laws and regulations. Degreed promptly investigates and notifies in case of personal data breaches, follows strict sub-processing guidelines, and maintains a robust privacy management system reviewed annually.

- ***Information Security Policy:***

The Degreed Information Security Policy focuses on protecting the confidentiality, integrity, and availability of Degreed information, assets, systems, and applications.
Information Security Policy applies to all individuals authorized to conduct business for Degreed and all systems, applications, and services essential for business operations or client services. Degreed utilizes a risk-based approach, conducts vulnerability assessments, penetration testing, and implements antivirus/antimalware solutions.
Led by the Information Security Officer, Degrees is focusing on governance, security assurance, and security operations to ensure compliance, security awareness, and continuous improvement. Degreed undergoes internal security audits annually, participates in SOC 2 Type II audits, and holds TISAX certification.
The policy emphasizes information security as a top priority for Degreed, aligning activities with commercial efforts, internal systems improvement, and effective communication to enhance the maturity and predictability of the information security program.

Information Protection

Degreed has stringent policies and standards in place to safeguard sensitive information from unauthorized disclosure. Here are key points related to information protection:

Data Loss Prevention Controls:

- Access to service data requires remote access using Virtual Private Network (VPN) and Remote Desktop Server (RDS).
- Strong access controls are enforced for remote access to service data.
- Various restrictions and role-based access control (RBAC) are in place to prevent unauthorized actions like FTP access, cloud storage access, and more.

Password Control:

- Passwords must adhere to strict standards aligned with NIST publication SP 800-63b.
- Users must acknowledge and comply with password standards outlined in Degreed's policies.

Data Encryption:

- Encryption is mandatory for protecting data at rest and in transit.
- Strong encryption mechanisms are used for data at rest and during transmission over public networks.
- Specific protocols like TLS encryption for emails and SFTP/FTPS for file transmission are required.

Remote Data Access:

Degreed employs a jump server solution to secure client data access. Key aspects of remote data access:

Jump Server Solution:

- Client data access is restricted within a secure Azure server environment.
- Authorized employees connect to the Azure Remote Desktop Server (RDS) via VPN with two-factor authentication.
- Access to specific resources and data is controlled based on EntraID role-based group permissions.
- Production data, including client SFTP files, can only be accessed through the RDS.

Technical Controls:

- Various restrictions are in place to prevent data transfer to personal devices.
- User accounts have automatic lock and logout features for security.
- DLP restrictions and technical controls ensure secure data handling within the RDS environment.

Risk Management:

Degreed employs a risk-based approach to information security and decision-making, as outlined in Degreed Risk Management Policy. Key aspects of Degreed's Risk Management:

- The policy aims to identify, assess, and mitigate risks to critical information assets while ensuring compliance with relevant regulations and standards.
- Degreed follows the Center for Internet Security Risk Assessment Method (CIS RAM) for its technology assets to assess security posture against best practices.
- Risk assessments are conducted during various circumstances, including system changes, supplier evaluations, and external changes affecting Degreed.

Roles and Responsibilities

- Various roles are involved in the risk management process, such as Senior Leadership, Information Security Officer, Governance, Risk, and Compliance (GRC) team, and Application Security (AppSec).
- Risk Owners and Control Owners play crucial roles in managing and implementing risk mitigation strategies.

Risk Prioritization and Reporting

- Risk prioritization considers factors beyond risk classification, including expectancy score, impact, compliance requirements, and business criticality.

- The risk assessment report includes details like asset class, threats, vulnerabilities, controls, risk scores, and treatment priorities.

Continuous Improvement and Reporting

- Reporting mechanisms are used to report risk reduction, data inconsistencies, and the effectiveness of mitigation strategies.
- Regular reviews and updates ensure that risk management processes remain effective and aligned with Degreed's objectives.

This comprehensive approach to risk management ensures that Degreed can proactively identify, assess, and address risks to safeguard its critical information assets effectively.

Incident Response:

The Degreed Incident Response Plan describes roles, responsibilities, and procedures for responding to information security events and incidents. Outlines detection, evaluation, containment, restoration, evidence collection, communication, root cause analysis, and after-action reviews.

Objectives:

- Protect information resources by reducing and containing security incidents.
- Ensure quick restoration of Degreed assets.
- Fulfill obligations to policies, contracts, and laws while preserving evidence.

Activation Criteria:

- Guides responses to security and privacy events and incidents.
- Activates the response plan when an event is defined as an incident.

Regular Auditing and Review:

- Annual audit to monitor processes and tools' effectiveness.
- Testing includes simulated exercises for incident response capabilities.

Reporting Security Events:

- All Degreed users must report suspected security and privacy events promptly.
- Detailed steps for reporting security and privacy events are communicated with all employees and contractors within annual Security Awareness Training.

Degreed Policies Overview

- **Technology Use Code of Conduct**

  The Degreed Technology Use Code of Conduct outlines the acceptable activities and behaviors related to the use of Degreed resources, covering various topics such as computer and network access, internet usage, cloud computing services, electronic communications systems, physical security, data security, device protection, and security event reporting. This policy applies to all individuals with access to Degreed's systems, including employees, contractors, consultants, and temporary workers. Users are required to review and acknowledge this Code of Conduct annually. The document also includes information on security training for technology teams, emphasizing the

importance of secure development training to stay updated on security practices and threats.

- **Identity and Access Management Policy**

  The Degreed Identity and Access Management Policy establishes requirements to manage access to Degreed information resources in alignment with business and security needs. It covers creating electronic identities, authentication, authorization management, and account de-provisioning. The policy applies to all individuals accessing Degreed systems, including employees, contractors, and consultants, ensuring secure access to network resources and applications. Key aspects include regular access reviews, principle of least privilege, and alignment of user access with job roles. The policy involves various systems like Configuration Management, IAM, Change Management, and Disaster Recovery, each playing a crucial role in maintaining secure access. Additionally, the policy includes standards for antivirus/antimalware, patch management, and access control, emphasizing unique user identifiers, role-based access controls, and privileged access management. Regular reviews and updates are conducted to ensure policy relevance and effectiveness.

- **IT Asset Management Policy**

  The Degreed IT Asset Management Policy establishes requirements for managing IT equipment and software, including procurement, documentation, tracking, and disposal of IT assets. Policy applies to all Degreed staff and assets.
  Degreed utilizes Mobile Device Management solutions for organizing, managing, and tracking IT assets.Includes various asset classes like desktop workstations, laptops, network appliances, and more.
  Asset Tracking involves installing asset tracking software or agents, tracking cloud services, and managing asset value.
  All Degreed IT assets are company property and subject to monitoring; The policy ensures proper management, tracking, and security of IT assets within Degreed, safeguarding sensitive information and maintaining compliance with corporate standards.

- **Endpoint Vulnerability Response Process**

  Degreed's Endpoint Vulnerability Response Process involves monitoring and responding to alerts and issues generated by endpoint protection solutions. Here is an overview of the key points in the process:

  - The IT team uses MDM solutions like Microsoft InTune and Jamf Pro for policy management and patching.
  - SentinelOne is deployed as an active EDR solution in "Protect - Kill and Quarantine" mode for alerts.
  - EDR triggers automatic responses to malicious or suspicious activities, generating alerts and IT service management tickets.
  - Incident alerts are reviewed and remediated within one business day.
  - Weekly IT tickets track the review of other endpoint vulnerabilities identified by the EDR.
  - Automox patching policies automatically address critical and high vulnerabilities.

Additionally, the process includes standards for antivirus/antimalware, patch management, access control, risk management, and continuous improvement. The remediation timeline for vulnerabilities is based on severity, with critical issues requiring immediate attention and regular ticket reviews to ensure timely resolution. The process also involves continuous monitoring, vulnerability assessments, and configuration changes. Endpoint hardening practices are implemented to ensure secure workstation usage, including hardware and software asset control, antivirus deployment, access control, encryption, and software patching. Automated testing processes are in place to scan code for vulnerabilities and code quality, with daily scans and review processes to address identified issues.

- **Information Classification Policy**

  The Degreed Information Classification Policy defines the types of information handled by Degreed, emphasizing confidentiality, integrity, and availability principles. Details how information within the company is classified based on the confidentiality of the information (Sensitive, Confidential or Public) and the handling of each type of information. It applies to all information maintained by Degreed and its employees, contractors, and partners, outlining controls to safeguard information.
  Employees must classify information appropriately, distribute it on a need-to-know basis, and follow protection measures. Unauthorized reproduction or destruction of company data is prohibited, and temporary access to information should be tracked and revoked when no longer needed. Information should be stored in Degreed's cloud storage, and local storage used temporarily only.

- **Data Retention Policy**

  The Degreed Data Retention Policy focuses on consumer/customer data, outlining that client data is retained for the duration of the contract with Degreed. Specific scenarios for data removal include learners requesting profile removal, employees leaving organizations, and organizations discontinuing services. Learners can remove their profiles at any time, with personal information promptly deleted upon request. When an employee leaves an organization, proprietary information is removed, and profiles are set to private. If a personal email is not provided, profiles remain for 90 days before being anonymized. The policy ensures data is securely stored in Azure environments and emphasizes individualized handling of data removal requests.

- **Cryptography Policy**

  The policy provides guidance on encryption technologies to protect confidential or sensitive information within Degreed and ensure compliance with contractual requirements.
  Encryption is mandatory for "Sensitive" or "Confidential" information. Applies to all Degreed assets like laptops, desktops, mobile devices, Azure network services, and business systems.
  Encryption algorithms must meet NIST standards.

Policy defines specific encryption standards for outbound email, data at rest, data in transit (web and external file transfer), password hashing, key management services, and certificate authorities.
Non-secure protocols like HTTP, FTP, Telnet, SNMP, and older TLS versions are prohibited.

- **Change Management Policy**

  The Degreed Change Management Policy outlines the approach to manage changes within the organization effectively and predictably. The policy distinguishes between software, infrastructure, documentation, and internal IT changes.
  Policy defines workflows for requesting and tracking changes. Evaluating changes for impact, including security and privacy considerations.
  Changes are approved based on risk.
  Implementation planning, scheduling, testing, and rollback procedures are conducted as needed. Changes are verified after implementation.
  Policy outlines emergency change procedures.
  Post-mortem reviews on failed changes are conducted and outcomes are documented.

- **Network Security**

  Degreed cloud resources are protected by Network Security Groups (NSG), Web Application Firewall (WAF) and Azure Front Door. The Information Security team conducts bi-annual reviews of firewall configuration, including office location firewalls, Azure Web Application Firewall (WAF), and Azure Network Security Groups (NSG). Here is an overview of the firewall review process at Degreed Network Security:

  - Office Location Firewalls:
    - The IT team logs into each office location router to extract current firewall settings for review.
    - Settings are reviewed by Security Analyst and any necessary changes are submitted via the IT portal for administration.
  - Azure Web Application Firewall (WAF):
    - Security Analyst reviews WAF configuration and rule sets to detect any changes and make sure Degreed follows industry best practices to avoid common web application threats.
    - Changes are validated, confirmed, and submitted for any required adjustments.
  - Azure Network Security Groups (NSG):
    - NSG rulesets are exported, reviewed and changes are documented.
    - Results are reviewed with SMEs, and tickets are submitted for necessary modifications.

  These processes ensure the continuous monitoring and maintenance of firewall components to enhance network security at Degreed

- **Physical Security Policy**

  The Degreed Physical Security Policy establishes security measures for Degreed office locations, focusing on access control and physical safeguards.

Degreed offices are secured with access cards or keys. Cards are inventoried and periodically reviewed.

Employees report lost or stolen cards or keys immediately and the IT team disables them. Access cards or keys are also disabled during employee off-boarding.

Fire and safety inspections completion is confirmed annually.

Office entrances are monitored with CCTV and footage is retained for 90 days where possible.

Additionally, the policy outlines responsibilities for facility managers and the IT team, compliance measures, and related documents. It emphasizes the importance of physical security for remote work office locations, covering access controls, visitors, printing, network security, and more. Violations of the policy may lead to disciplinary actions, including termination. Employees are expected to follow physical access requirements, report violations, and adhere to security measures for workstations and document storage.

- **Secure Development Policy**

  The Degreed Secure Development Policy focuses on rules and principles applied to software development and engineering activities related to applications and services offered for client use. Key points include source control versioning, third-party library usage, developer training, coding standards, software development lifecycle, code peer review, and vulnerability scanning with remediation processes. Vulnerabilities are identified through various security testing methods and remediated following the Degreed Risk Management Policy. The policy emphasizes secure development practices, such as the principles of least privilege and segregation of duties, applicable to all developers, both internal and external, and outsourced development. Additionally, the policy ensures that network architecture and design are peer-reviewed, high impact changes follow approved processes, engineers are informed about threats, and system design includes risk assessments.

- **Vulnerability Management Standards**

  Degreed's Vulnerability Management Standards establish protocols for identifying, assessing, prioritizing, managing, and mitigating vulnerabilities within its IT systems and infrastructure. The purpose is to safeguard sensitive data, maintain IT resource integrity, ensure availability, and comply with regulatory requirements. These standards cover all systems, networks, applications, and databases owned or managed by Degreed, including those hosted internally and by third parties. The process includes maintaining detailed vulnerability records, periodic reporting to senior management, security awareness training, simulated phishing campaigns, and continuous improvement through regular reviews and updates. The standards also encompass risk management, secure development practices, audit controls, and enforcement measures.

- **Logging and monitoring**

  The logging and monitoring processes at Degreed are comprehensive and essential for maintaining security and compliance. Here is an overview of Degreed's logging and monitoring practices:

Logging:

- Access Logging Process:
  - User access logs and privileged activities are aggregated in Azure Log Analytics for monitoring.
  - Logs include internal and third-party application access, authentication methods, failed login attempts, source IP logging, and timestamps.
- Security and Event Logging:
  - Logs record user activities, exceptions, faults, and security events like login attempts and system changes.
- Performance Logging:
  - Logs measure and monitor system performance and availability.
- Accuracy and Retention:
  - Logs are classified, protected, and retained for forensic investigations.

Monitoring:

- Real-Time Alerts:
  - Alerts are configured to detect suspicious access activities and anomalies in real-time.
  - Immediate alerts are generated for unfamiliar login patterns or suspicious activities.
- Log Management:
  - Security logs are stored, analyzed, and reviewed monthly using Azure log analytics tools.
  - Logs are stored for 2 years with encryption in transit and at rest.
- Compliance Monitoring:
  - Regular monitoring of usage logs and security event logs is conducted to ensure compliance and detect suspicious activities.

- **Business Continuity Policy**

The Degreed Business Continuity Policy establishes a systematic approach to business continuity management, backup/recovery requirements, and plan testing to ensure service availability and minimize disruptions.

Policy establishes a commitment to organizing, managing, and implementing sound business resiliency practices and aims to avoid/minimize loss of service to clients and adverse impacts on client data during disruptions.

This policy covers all Degreed personnel, assets, and information security operations.

Policy Highlights:

- Adoption of well-defined plans, redundancy in teams and infrastructure, and backup arrangements for business systems.
- Conducting an annual Business Impact Analysis (BIA) to assess critical processes and services.
- Creation of a Business Continuity Plan with specific requirements, including a Crisis Management Team, plan activation criteria, roles and responsibilities, and recovery objectives.

- Planning against scenarios like loss of facility, IT application, technology, and staff unavailability.

Responsibility:

- The Governance, Risk & Compliance Team is responsible for maintaining the policy.
- Approval is jointly done by the Chief Technology Officer and the Chief of Business Operations.

- **Third party risk management policy**

Degreed's Third-Party Risk Management Policy focuses on managing information security risks associated with third-party suppliers. The policy includes requirements such as evaluating third parties' security controls, establishing mutual non-disclosure agreements, and utilizing relevant contractual instruments. Additionally, the policy mandates regular vulnerability assessments, annual penetration testing by independent third parties, and the tracking and remediation of identified vulnerabilities. These measures aim to ensure the security of Degreed's systems and applications in alignment with industry standards and best practices.

Degreed Customer Data Collection, Usage, and Retention Overview

Data Collection:

- Data Minimization: Personal data processed by Degreed is limited to what is necessary for the agreed-upon purposes.
- Accuracy: Personal data is kept accurate and up-to-date, with steps taken to rectify any inaccuracies.
- Storage Limitation: Data is retained only for the necessary duration based on the purposes of processing.
- Workstation Usage and Security: Employees are responsible for protecting devices and handling company data, following specific guidelines to ensure security.

Data Usage:

- Lawfulness & Fairness: Data processing is done in compliance with Data Protection Laws and based on valid legal bases.
- Transparency: Data subjects are informed about the processing of their personal data as required by Data Protection Laws.
- Purpose Limitation: Data is collected for specific, legitimate purposes and not further processed in incompatible ways.

Data Retention:

- Data Removal: Client data is retained for the duration of the contract with Degreed and is removed in specific scenarios like learners leaving Degreed or employees departing an organization.
- Data Backups: Degreed utilizes Azure SQL for primary database backups, with a 35-day point-in-time restore policy and weekly backups retained for 90 days.

- FTP Server File Retention: Client files provided to Degreed are retained for 90 days, reporting files for client use are available for 90 days, and internal client reporting files are deleted after 1 year.
- Logs Retention: User access and alert logs are retained for 1 year, ensuring historical data availability for security incidents.

This overview highlights Degreed's approach to customer data collection, usage, and retention, emphasizing data protection, transparency, and compliance with relevant laws and policies.

FAQs

1. What customer data do we collect?

For SaaS deployments, Degreed collects the following type of
customer data: (i) name, email, job title, employee ID (Optional). (ii) Learning data.

2. *Where is customer data stored?*

Degreed stores customer data in secure Azure environments using defined storage solutions, retaining data for the duration of the contract with Degreed. Here are some key points regarding Degreed's customer data storage:

- Customer data is housed in secure Azure environments with consistent storage solutions.
- Data is retained for the duration of the contract with Degreed.
- Personal information is removed when a learner requests profile removal.
- Degreed utilizes Azure SQL for its primary database, with backups replicated to paired data centers for protection against outages.
- Client files provided to Degreed are retained for 90 days for client support.
- User access logs and privileged activities are aggregated in Azure Log Analytics for monitoring and security purposes.

Degreed ensures compliance with data protection principles, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.

We store customer data on Azure Cloud Platform’s servers located in the United States, EU and Canada.

3. *What additional contractual protections do we provide with respect to personal information and customer data storage, processing and transfers?*

We offer our customers a Data Protection Addendum (DPA).

4. What are our retention policies with respect to customer data and personal information?

Information we collect or generate is retained in accordance with our contractual commitments to our clients and any statutory or regulatory requirements.