Mentor & Match

Cybersecurity Policy



INTRODUCTION

Mentor & Match is a transformative virtual mentoring platform designed specifically for community colleges, aiming to bridge the gap between students and valuable mentorship opportunities. At its core, Mentor & Match recognizes the pivotal role mentorship plays in student success. Community college students often face unique challenges and uncertainties as they embark on their higher education journey. Mentor & Match seeks to address these by pairing students with experienced mentors who can provide guidance, support, and real-world insights.

Through utilizing Mentor & Match, students can benefit from the wealth of knowledge and experience that mentors bring to the table. These mentors are often professionals from the local community, alumni, administrators I, classified professionals or faculty members who can provide students with academic advice, career guidance, and personal development strategies. By fostering these meaningful connections, Mentor & Match not only empowers students to navigate the complexities of community college but also ensures a smoother transition to their future academic and professional endeavors. It's a platform that not only enhances the educational experience but also strengthens the ties between the college and its surrounding community, creating a nurturing and supportive environment for all involved.

CLOUD SECURITY

Cloud Classification & Configuration

- Our software solutions are hosted on Microsoft Azure public cloud.
- We are a provider of SaaS solutions for Higher Education institutions that include web and mobile applications hosted on Azure.

ACCESS CONTROL

Policies & Procedures

- Policies are reviewed annually or upon any environmental change.
- Capability to create the Individual and School Group Accounts for the institution service staff and individual accounts for students.
- Does not support guests or temporary accounts.
- Separately, the company uses Azure Active Directory for the members of the company that supports Individual, group, system, etc., accounts.
- Has a separate administrative application that is used to set up separate tenants by customer and to create the designated school administrator access.
- Uses Microsoft Azure access control and security services to secure access. Sourcecode is stored in Atlassian BitBucket with limited access the company uses DevOps CICD pipelines to deliver the code in an automatic way to the production and staging environments.
- No personnel have direct access to the data or code in the production environment.
- Access is revoked as soon as the Information Technology Team is notified by the user's manager, by the project lead for contractors, business partners, and third parties, or by the Customer Success/support teams for customers.
- Does not implement any temporary or emergency accounts.
- Transition of data between the web and API servers and clients is secured by SSL/TLC protocols.
- We do not require certifications for system users and administrators.
- All users are under the tenant. The solution does not require everyday login for the tenant administrators or staff. The policy is not applicable for our automated solutions. It

does not require consistent validation of login of the staff. In our Quarterly Business Reviews (QBR), we generate a report for the tenant to review.
- The solution will log out sessions after 30 minutes of activity and require users to re-log in.

ACCESS CONTROL - ACCESS ENFORCEMENT
- Uses Microsoft Azure access control and security services to secure access to the solution. The company restricts access to Azure resources only to Azure admin. Azure admin assigns limited access for resource provision or maintenance to the personnel for a well-defined time and based on least privileged access principles.
- Microsoft Azure Active Directory prevents unauthorized access to any of our solutions.
- Customers oversee their own customer/user data.
- A policy is in place to notify customers if inappropriate access has occurred.

ACCESS CONTROL - UNSUCCESSFUL LOGON ATTEMPTS
- We have password requirements in place and are implementing lockout processes at this time.
- Web application requires a minimum of 6 characters: 1 upper case, 1 special character and 1 numeric.

AWARENESS AND TRAINING
Policies and Procedures
- Information and Security Awareness Training policy will be implemented as part of the onboarding process.
- Upon completion of the training, all employees will sign a completion/acknowledgement form which will be stored in their Human Resources record.
- All current personnel have signed individual NDA's and confidentiality agreements, this will be included in onboarding packets for future employees.

AUDIT AND CONTROL
Audit and Accountability
- User accounts are audited on a quarterly basis.
- Using the third-party tools to test our Microsoft Azure-hosted solutions by implementing the best practices and guidance.
- Audit results are provided to users upon request.
- Audit records will be maintained in a centralized log management system in accordance with organizational record retention policies.

CONTROL ASSESSMENT AND AUTHORIZATION
- Will provide the health report of the Azure resources that are used or the solution, upon request.
- Will provide the annual risk assessment review associated with data governance requirements, upon request.

CONFIGURATION MANAGEMENT
Policy and Procedures
- We utilize the Atlassian Jira Software for tracking all solutions issues.
- We have implemented Atlassian Jira Software to assign priority to all issues, bugs and enhancement requests from our customers.
- Customer reports the issue to the Customer Success team.

- When the issue is resolved, the customer is then notified of the update along with any user training that may be applicable.
- All application updates are handled through API's to only bring the updated code into the production environment.
- Our access controls follow the principle of least privilege – meaning users are only authorized access at the minimum level required for their role. Only authorized personnel would have access and install pre-authorized software into our environment.

CONFIGURATION MANAGEMENT

Policy and Procedures

All application updates are handled through API's to only bring the

- Our access controls follow the principle of least privilege – meaning users are only authorized access at the minimum level required for their role. Only authorized personnel would have access and install pre-authorized software into our environment.
- The application is a very lightweight application. It has very little customer data that is saved in the system.

CONTINGENCY PLANNING

Information System Backup

- Our solution infrastructure has Azure zone redundancy. Locations are all in the Eastern United States geographic area.
- The solution is designed for redundancy in Microsoft Azure to recover in an orderly and timely manner.
- The solution has separate tenancy for each college and all their data.

IDENTIFICATION AND AUTHENTICATION

Organizational Users

- Management determines the access and authorization requirements for all employees, contractors, business partners or suppliers.
- Tenant customers manage their own user access and restrictions.
- The access must be authorized prior to any access to the application.
- We require an annual review and updates for our access policies for all system users and administrators.
- To date we do not have customers currently requiring Single Sign On,

AUTHENTICATOR MANAGEMENT

To date we do not have customers currently requiring Strong Multifactor authentication, but we have the ability to implement Azure Active Directory to accommodate the customer to accept their authorized users.

- To date we do not have customers currently requiring third party identity assurance services, but we have the ability to implement once our due diligence is complete in vetting the software according to Mentor & Match.
- Within next 60 days we are implementing OKTA for Multi Factor Authentication (MFA) and Single Sign On (SSO)A system administrator from the IT team will be able to assist the user to manually unlock the account when necessary.\We anticipate customized tenant requirements for each of our customers in the security incident response plans.
- Given the recent migration of our application to Microsoft Azure, we
- All security incidents will be monitored and quantified to be proactive to mitigate any security incident trends.

- All statistical information for security incident data is shared with our tenants upon their request.
- Tenant data is separated by tenant, so only tenant data would be produced in response to any legal subpoenas or requests.

SYSTEM AND COMMUNICATIONS PROTECTION

Encryption

- Microsoft Azure manages all the encryption in our databases.
- Our solution environment separates production data from all other non-production environments. Production data is only accessible via API's calling data from the web application or the mobile application.
- Only authorized C Level personnel have access to the production database.

SECURITY FRAMEWORK

Organizational Security Framework

- To manage cybersecurity risk and protect critical assets, our company has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework as an information security policy.

INCIDENT RESPONSE

- We anticipate customized tenant requirements for each of our customers in the security incident response plans.
- Given the recent migration of our application to Microsoft Azure, we are in the process of creating formal security incident response plans tailored to our multi-tenant cloud environment.
- All security incidents will be monitored and quantified to be proactive to mitigate any security incident trends.
- All statistical information for security incident data is shared with our tenants upon their request.
- Tenant data is separated by tenant, so only tenant data would be produced in response to any legal subpoenas or requests.

SYSTEM AND COMMUNICATIONS PROTECTION

Encryption

- Microsoft Azure manages all the encryption in our databases.
- Our solution environment separates production data from all other non-production environments. Production data is only accessible via API's calling data from the web application or the mobile application.
- Only authorized C Level personnel have access to the production database.

Mentor & Match

www.mentorandmatch.com

info@mentorandmatch.com

(877) 211-8504