10/02/2021

Tribu Data Security Document

Objective

The document incorporates all the security information issues of the Tribu company and its products in accordance with external audits and tests performed during the current calendar year.

General

Tribu is committed to protect the privacy of its customers in accordance with the Privacy Protection Regulations of the Israeli Ministry of Justice - Privacy Protection (Information Security) Regulations, 2017
(https://www.nevo.co.il/law_html/law01/501_600.htm)
accordingly, the Company undergoes annual auditing information security and penetration testing in order to verify compliance.
Tribu is working with the Ministry of education and is recognized as an official supplier of the office, which requires us to comply with the limits security and Privacy at the highest level.

DataBase

Tribu is holding a Database of information legally registered at the Ministry of Justice.
The database is classified at high security.
the Database manager assignment

Secured development

carries	Explanation	Comply	notes
Secured Development Policy	The organisation needs to guide the developer in the process of secured development relevant to the technologies being used. there is a need to document these guidelines.	✔	Secured Development Policy
testing Input validation: Make sure the software checks any data coming from the user, in forms, cookies, query strings, HTTP headers	Any variable containing information coming from the user must be checked to make sure it does not contain malicious code, which can damage information in the system or computer running the software Or browsing to the site. Test functions should relate to tests such as input type, encoding, special symbols and keywords	✔	
tests input (input validation) should be documented and warn in case of invalid input	when the system detects input as invalid, it has to warn the user and simultaneously record the data in a log file and / Or a table that will allow the user to be questioned. The test must be performed on all pages	✔ Invalid	input is monitored only on login and a log is maintained. All operations in the system are protected in the permissions system
There is a permissions Access policy to tables in the database by user types and roles in the system	Applicable user should have access to necessary objects (tables, functions, etc.) And not for all objects in the database. Do not use the permissions of admin / root / sa user application	✔	Permission matrix Organizations are not exposed to information from other organizations, each organization is a separate environment.
Encryption	Use of known encryption mechanisms and not those written proprietary	✔	Attached
Use of TLS 1.1 / 1.2 only	Encoders other than TLS 1.3 / 1.2 should be avoided. Tests must be performed in a TEST environment before moving to production.	✔	

Handling sensitive information

carries	Explanation	Comply	notes
detection and treatment of sensitive data: passwords, login login info to server and database, private data of users, access to externa resources	login server and database must be encrypted by a dedicated mechanism or as part of the operating system. Personal Information and Sensitive , must be stored encrypted in the database	✔	Attached
Do not store confidential data which is not essential to the functionality of the system (such as credit cards, medical information)	does not retain un-necessary information in the system, i.e. information that is not essential for the system to operate.	✔	
In case of using payment system, It should be done through a service which is PCI compliant and comply with SEC requirements, privacy protection	should use an external payment system conforming which is PCI compliant approved by the privacy protection authority and Do not keep the payment details on your site.	✔	not relevant to the

Identification and passwords

carries	Explanation of	Comply	notes
Entering a user name and a personal password	system Does not reveal passwords on the screen	✔	
Entering a username and personal password	does not automatically complete the identification details	✔	
Password Length	Minimum length - 7 characters	✔	8 characters
Complex password	Password will consist of letters and numbers	✔	8-15 characters including uppercase and lowercase letters, a number and a special character. Special characters: @!% $ & #
"Forgot password" mechanism	A password reset link will be sent to the email / phone under the sole control of the user	✔	
Entering a wrong password twice	Using a captcha	X	No captcha support
Entering an incorrect password 5 times	Blocking a user And disconnection from the system	✔	
One password change every 180 days	Setting up and enforcing password change every 180 days	✔	
Old password usage policy The	system must block the use of previous passwords. Save password history, up to 5 passwords	✔	
2 factor authentication	Use additional verification mechanism	X	

Session Management

Subject	explanation	Comply	Notes
Idle Timeout mechanism	Idle Timeout mechanism must be maintained by terminating the user's session after 60 minutes of inactivity in	✔	
reconnection after the system down	when there is an unresponsive system or restarting the Web server, you need to login again	✔	
disconnecting Session	Disconnect the Session will be happen at the expiraton of the Session on the server side, rather than just moving the client to the login page.	✔	

Servers and communication

subject	explanatory	Comply	notes
operating system update and database, servers	Operating system and services should be updated to the latest version. The period of time in which an update will be performed must be specified. It is recommended to update every month	✔	
Use latest versions of the development language including third party services and open source.	Use the version that contains the latest information security updates of the main version (magor release) on which the system is developed, including products such as wordpress moodle, etc.	✔	
Open ports	should check Which ports are open. Make sure there are no unnecessarily ports open	✔	Attach
a WAF application to WEB servers	for website protection, add a layer of Web Application Firewall service that will allow protection of the website (in addition to FireWall). This layer monitors and blocks attacks at the application level and prevents abuse of the HTTP / S	protocol ✔	We use the service Incapsula
AV should be installed on all Windows servers AV should be installed on Linux servers to which users upload files and make sure the AV is updated with certificate regularly		✔	
Are there firewalls and components of IPS to prevent attacks on the application?		✔	Incapsula, AWS
configuration of the	an explanation of the existing solution	✔	AWS auto scaling

servers include network availability to ensure continuous access to implementation of			
Server location			AWS Frankfurt

Documented logging and warnings

theme	explanation	Comply	notes
Maintain complete documentation and system warnings about unauthorized actions	Documentation of application logs, of the servers (such as IIS, Apache) and of the information security systems such as WAF, IPS, FW, antivirus	✔	
Documentation of actions in a log containing user details	Action must be documented with the detailed of the executor	✔	
logs should be maintained for a period of 24 months		✔	

Handling cyber incidents

topic	explanation	Comply	comments
Is there a cyber security manager full time		X	
Is there a procedure for handling events of cyber		✔	Attached
Does the cyber event handling policy being examined at least once a year?		✔	
Is there a Data Security Procedure in the company		✔	Attached
When do you inform your customer on a cyber event?		✔	Up to 8 hours since discovered

Standards

Tribu adapted the privacy protection regulations of the State of Israel.
The system is installed on Amazon servers in Frankfurt and therefore meets all the server security standards.
Amazon meets the following standards:
ISO / IEC 27001: 2013, 27017: 2015, 27018: 2019, and ISO / IEC 9001: 2015
Full list and supported areas -
https://aws.amazon.com/compliance/iso-certified

GDPR standard - Although we do not officially have a GDPR standard certificate, the system complies with the essential definitions in the standard.
We do not pass on user information to any third party, we do not have advertisements, we allow users to delete their account without the ability to recover by contacting the support department, we do not engage in marketing activities that are not directly related to the trivial activity.

Previous Cyber Events

Tribu experienced a cyber incident in January 2020. The
event revealed a security vulnerability that allowed access to student's hourly reports for a limited time even to unauthorized users.
The incident was handled immediately and a permanent solution was implemented shortly after.
The main problem was in the asynchronous operation of exporting reports:

1. creating a report in the system
2. Clicking the export button - producing the report on the server side in the background.
3. When the report is ready - send a notification to the user with a link to the report.

The link to the report was active for 24 hours and without user verification.
The fix was shifting to a synchronous operation, so that reports are not stored at all on the server but are sent as a response to the export operation.
Attached is the incident investigation.