Supporting Policies and Statements

Licensor:

LTO Success Group Pty Ltd (“RTO Software”)
ABN: 35 741 076 779

PO Box 7511,
Gold Coast MC, QLD 9726

Introduction

LTO Success Group Pty Ltd ("RTO Software", “our”, “us”) provides an enterprise education management software called TEAMS. This software is web based and is used and applicable to a wide variety of education businesses and individual customers. The TEAMS software applications is also further customised for a variety of education clients (“client”, “you”, “your”) for use.

This document is to be read in conjunction with the TEAMS Licence Agreement and is applicable to all current clients of TEAMS.

This document is made up of Seven individual documents. Each of these documents and policies may be updated together or individually as appropriate..

TEAMS clients and other relevant and interested parties will be notified of these changes and amendments as they come into effect. A copy of this document is available online at the following address - https://www.rtosoftware.com.au/Supporting-Policies

These policies and statements are applicable to all clients that continue to use and hold a current licence for using the TEAMS Software.

The policies and statements contained herein are

1. Privacy Statement – Schedule One
2. Backup Policy – Schedule Two
3. Data Security Statement – Schedule Three
4. Security Breach Policy – Schedule Four
5. Support Process Statement – Schedule Five
6. Data Release Policy – Schedule Six
7. Cybersecurity Policy - Schedule Seven

Please contact our support team if you require any clarification or further details about any of the schedules mentioned above.

You may also report any errors or omissions in this document to our support team and we will do our best to address them as soon as we can.

The contact details are:

via email - support@rtosoftware.com.au

via phone - 1300 850 585

via post - PO Box 7511, Gold Coast MC, QLD, 9726, Australia.

Schedule One

Privacy Statement

Last updated: 15th Feb 2024

Introduction

Any information that you provide through our websites or your web application sites (such as TEAMS), the storage and use of such information is governed by the RTO Software Privacy Statement.

This document sets out our policies relating to the collection and use of your personal as well as business application specific information. This document is to be used in conjunction with the Software Licence Agreement (if applicable) and any other documents that are mentioned within this statement.

Contents

Your personal information is important to us:

We recognise that your privacy as well as the privacy of information about your clients, your affiliates and any associated parties is very important and that you have a right to control and access such information. We know that providing personal information is an act of trust and we take that very seriously. The following sections set out how we handle and protect your personal information and safeguard your privacy.

.....

Support Sites and User Accounts:

RTO Software has implemented a Support Site that is an online option to and interacts with other support staff to assist with RTO Software applications.

All RTO Software application clients are given User Accounts to our Articles & Forums sites at the time of product implementation. At signup, you will be prompted for information such as your name, contact details, email address, address details and company details

.....

How we collect information about you:

There are three main ways we collect information about you:

1) If you are not or do not log in as a RTO Software client or do not access our application sites –

Whenever you visit any of our websites, our servers automatically record information about your usage of our sites, such as the time of the visit, its duration and the pages you visit. We also log your IP address to uniquely identify you.

This information is captured to help us understand what parts of our Sites our users enjoy the most and to help us ensure that advertisements or articles on our sites are most directly relevant to your interests. If you have not identified yourself on our sites, such as by registering for Membership or logging in as a member, or visiting one of our application websites, the information we collect about you remains anonymous.

2) If you log in as a client / member on our support and articles sites –

Once you have a User Account for our Customer Support site, we collect personal information about you in order to provide you with the full benefits of Membership. When you first register for Membership, we collect information from you such as your email, name and suburb, and will continue to add to your member profile as you interact more on our Sites, for example, if you update your details or subscribe to our newsletters.

3) If you login via one of our application sites and access one of our paid services –

When you register to receive our paid services, for example, TEAMS, Work Flow Manager or any other applications and products, we may collect application specific information such as names of your clients, your affiliates, your business details, email addresses, logs about communication with your clients etc. This information is governed by strict confidentiality and security and our Software Licence Agreement, Backup Policy, Data Security Policy, Security Breach Policy and Staff Code of Conduct should be read to further understand the extent of measures and responsibility that we undertake to keep that information secure.

.....

How we preserve your privacy:

We understand that even with our Privacy Policy, some people will not feel comfortable disclosing personal information in order to become a RTO Software member. To use our Articles & Forums site you must be a RTO Software application client and at all times we respect and protect our clients information. We collect information in order to give our clients the most enjoyable and customised experience of the RTO Software sites as possible.

.....

How we use and disclose your information:

We will not disclose any information about you without your consent unless it is

- Required by law;

- We believe it necessary in order to provide you with a service which you have requested;
- We suspect that your use of the RTO Software sites are in breach of the Terms of Use relating to that Site;
- To lessen a serious threat to a person's health or safety.

We will never share your personal information with a third party or allow a third party to promote its products and services directly to you without your explicit consent.

We will never sell your information or disclose it to third parties. We are further committed to safeguarding your information and will work to minimise all possible forms of threats that information and its use can pose a risk to your business or may constitute an infringement of your or your client's and affiliate's rights to privacy.

.....

How we communicate with our clients: service messages and promotional messages we send to you:

We send our clients service emails which contain important information about updates, changes and developments on the RTO Software Sites, such as if we have to take down a service for maintenance which we know you are currently using, or, if we have improved a service and want to communicate its new functionality to you. For you to continue to make the most of what's available through us, it is essential that we send these communications.

From time to time, we will send you memberonly offers from our carefully selected partners, email newsletters to which you have subscribed, and tell you about products or services we offer.

You can manage the type of information you receive from us by:

- updating your Membership profile;
- unsubscribing from the message you receive; or
- Emailing us on our privacy feedback form (please allow up to seven
- days for such requests to be processed).

.....

How we store your information and keep it secure:

We will take all reasonable steps to keep secure any information we hold about you and to keep this information accurate and up to date. Your information is stored on secure and protected servers that are stored in controlled facilities with access limited to authorised personnel.

In addition, our employees and the contractors who provide services related to our information systems are obliged to respect the confidentiality of any personal information held by us.

You can also play an important role in keeping your personal information secure by maintaining the confidentiality of any password and accounts used on the RTO Software Sites. Please notify us immediately if there is any unauthorised use of your account by any other Internet user or any other breach of security.

While, we will undertake all reasonable measures to keep your information secure, however, we will not be held responsible for events arising from unauthorised access to your personal information such as a password being disclosed by your staff or other such breaches.

.....

What do we do in the event of a security breach?

In the unlikely event that our server's or our Site's security has been compromised by an intrusion from an outside source, we will notify you immediately of the breach. We will then undertake immediate steps to stop the access to that Site or Server and find means to rectify the breach while the access has been stopped. For further details of our extent of liability and the sequence of actions taken, please refer to our Security Breach Policy.

.....

How you can access your information:

If you are a RTO Software client or a website member, you can contact the RTO Software support staff at support@rtosoftware.com.au to update

or enquire about your information. If you wish to know what other information we have gathered about you while you have been logged in to the RTO Software sites, you can request this information via support@rtosoftware.com.au. We will endeavour to respond to your request within seven days.

What to do if you have a problem or question:

If you make us aware of any ongoing concerns or problems with our RTO Software Sites, we will take these issues seriously and work to address these concerns. You can contact us via support@rtosoftware.com.au or our support hotline as given to you at the time of implementation.

.....

Changes to the Privacy Policy:

Our commitment to providing the finest in software and web based solutions means that we are constantly adding new sites and features to the RTO Software Sites. We will continuously review our Privacy Policy to ensure that it protects your privacy while supporting your user experience on the RTO Software Sites. We encourage you to keep visiting our Privacy Policy to see if any updates have been made.

.....

Further information on privacy:

For more information about privacy issues in Australia, visit the Office of the Australian Information Commissioner (OAIC). www.oaic.gov.au This site is a useful and recommended resource and provides guidance, and information about privacy laws and regulations in Australia..

Schedule Two

Backup Policy

Last updated: 12th August 2023

Introduction

We undertake a range of security and data backup policies to minimise the risk of a breach in client security and data integrity.

This document sets out our policies relating to the steps we undertake in backing up our clients' data.

Content

- What are RTO Software Backup Procedures?
- How do clients receive a copy of their backed up databases?
- Can we export data from the backup?

.....

What are RTO Software Backup Procedures?

RTO Software currently runs three backup procedures on each client database – a daily backup, a weekly backup and a remote backup.

The backup done daily occurs between 11pm and 4am in the morning. The backups start automatically taking a backup onto a NAS Server disk. Previous backups which are older than 15 days are removed.

The second backup procedure is the weekly backup done every Sunday between 1am and 4am in the morning. Backups that are older than 4 weeks are deleted and replaced with the new backup information.

The third backup procedure is that we copy your daily backup nightly to our remote servers in Brisbane through a private VPN. These copies are then deleted fortnightly on a rotation basis (if they are not used).

.....

.....

How do clients receive a copy of their backed up databases?

Yes, upon a written request, either via email or post (from an authorised and nominated representative) RTO Software can provide our clients with a copy of their backed up database via secure FTP access.

.....

Can we export data from the backup?

As long as the client has Microsoft SQL Server on their servers and have the copy of their backed up data they have the ability to export data. They may require assistance from suitable personnel with SQL experience to be able to restore and export or work with the data.

Microsoft also has made available Microsoft SQL Server Express Edition, which is a free edition of Microsoft SQL Server.

This product can be used to view and extract data to another format without having to have a licence or pay any charges for SQL Server. For further availability and information about this, please refer to Microsoft's web site https://www.microsoft.com/sql-server/sql-server-downloads

Please note that depending on your database size and other factors, the SQL Server Express Edition may not apply to you and you may have to purchase a suitable Microsoft SQL Server licence to use that database at your own premises.

Is there an alternative to Microsoft SQL Server format?

Yes, we can also offer our clients their data in a CSV format so that they do not have to use or deploy Microsoft SQL Server on their servers.

Schedule Three

Data Security Statement

Last updated: 7th January 2024

Introduction

The steps we undertake to keep your information secure and to ensure that our services provide you with ease of access while at the same time a high level of security are outlined in this document.

This document sets out our policies relating to the steps we take to minimise the risk of your information falling into the hands of unauthorised parties. This policy document should be read in conjunction with the Software Licence Agreement (if applicable) and any other documents that are mentioned within this statement.

Contents

.....

Secure Logins:

To ensure the highest levels of protection of user passwords and login information, we offer to clients that request it, a secure login to their application site. This helps ensure that your login and password information is sent via the https (secure) protocol and it helps to minimise the risk of a breach..

.....

Multi Factor Authentication (MFA)

Currently we have an OTP process for Mobiles and emails for all our users that login and use our software (client sites).

We also have MFA in place with AWS S3 and that's our only third party online service where we store client's data away from our own servers. It is being used for authenticating users or third party customer services (for both sensitive and non sensitive data).

.....

Protection of our external web servers:

We have two forms of external servers namely Web servers that provide http (web) services in the form of application sites and Terminal Services servers that provide access to our application sites via the remote desktop connection (RDP) protocol. In order to secure these servers from the threat of an intrusion, we have all external servers protected by firewalls in the form of a physical hardware firewall. This firewall is used as a filter through which all connections are routed.

.....

Protection of our data (internal) servers:

Our data servers hold all your information from the use of application sites. These data servers are protected from external access as they do not have an external IP. They are hence not accessible directly. The only way to access them is through our Terminal Servers and Web Servers. We further protect them by having a second firewall between the external servers and the internal servers.Further undisclosed security measures are also in place to deter any intruders from accessing our servers.

.....

Strong Password Policy:

We have a strong password policy providing further protection from unauthorised use. The passwords set for access to our external and internal servers have to be a mixture of characters, numbers and special characters (such as @, #, % etc) and have to be a minimum of 12 (twelve) characters long. We further have a policy of expiring these passwords on a monthly basis to ensure that they are always changing on a regular basis. This policy can be overridden by your own organisation's policies in the use of TEAMS. It is up to you in that case to ensure that passwords are not compromised.

.....

Account Lockout Policies:

We have an account lockout policy that upon 3 (three) unauthorised attempts, our servers automatically lock the account out and stop all access from that user account. This ensures that if someone were to find out an account name and try to guess the password, after only a limited number of attempts the account is locked out and the administrator is notified of the attempted breach. Administrators can then take appropriate remedial action.

.....

Restricted Access to Server Ports:

Except for HTTP, FTP, RDP, SMTP and other absolutely necessary protocols (as required from time to time), all our server's access ports are closed off. This is done to ensure that only services that are required and absolutely necessary for the operation of the server are available and open. This minimises the threat from hackers that use port scanning and other such tools to try and breach server security.

.....

Database level protection:

Every client's database is given a unique database owner username and password at the SQL Server level. This helps to ensure that in the unlikely event of our SQL server being intruded upon, the access is limited to only

the database that was breached and other databases cannot be opened with ease.

.....

Regular Backups and Data Protection:

Our entire set of databases is backed up on a regular and frequent basis (as per our Backup Policy). By undertaking regular end of day backups we ensure that any disruption or information loss in the event of our servers being unavailable or in the event of a server being affected by a failure is minimal. We also undertake off-site and secure backups on a regular basis. Please refer to our Backup Policy document for complete details of our backup processes.

.....

Schedule Four

Security Breach Policy

Last updated: 11th November 2023

Introduction

We undertake a range of security and data backup measures to minimise the risk of a breach in client security and data integrity.

This document sets out our policy relating to the steps we undertake in the unlikely event of a security breach. This policy document should be read in conjunction with the Data Security Policy and Software Licence Agreement (if applicable) and any other documents that are mentioned within this statement.

Contents

What is a security breach?

A security breach in simple terms is someone or something (such as a virus) gaining unauthorised access to restricted information (such as application or user data, web pages or other information). This breach may be detected or undetected and other factors such as the type of breach, the period that the breach occurred for and the likelihood of it reoccurring are also important considerations.

.....

What types of security breaches are there?

A security breach is primarily from any of the following 3 (three) sources –

a) External breach of security or intrusion – A third party or a third party agent (such as a virus) not linked to either RTO Software or your organisation has broken through the security measures in place and gained unauthorised access to our servers. This may include the external web and terminal services servers or the internal database servers.

b) Breach by RTO Software employee or affiliate – An employee or affiliate working for or on behalf of RTO Software gaining unauthorised access to a server that they were not authorised to use.

c) Breach by your organisation's employees or associated entities or persons – An employee or associate working for or on behalf of your organisation gaining unauthorised access to the data or website that they were not authorised to use.

.....

What are the various levels of security breaches?

Security breaches are primarily of the following three levels:

a) **Low risk** These are breaches that occurred but no user and application data information was exposed. The period of the breach may also be so brief that it may be physically impossible for any secure and private information to be transmitted to the unauthorised intruder. Such breaches constitute minimal risk to the data and the integrity of the information held. These breaches are not considered a serious threat and do not affect the data held on the servers.

b) **Medium risk** – These may be breaches that occur once only where some data was transmitted and some information was captured by the intruder. This may include user specific information or information

pertaining to specific sections of the data held. Such breaches constitute a serious risk.

c) **High risk** – These may be breaches that are caused over repeated attempts (possibly over a number of days) and with a sustained data access. This may include data, reports and other cumulative information being captured by the intruder. This may include a complete information store being downloaded or otherwise compromised by the intruder. Such breaches constitute an extreme threat and are considered a high level risk.

.....

How can you protect yourself from a security breach?

Security breaches in the form of hackers or third parties or viruses or spyware constitute only a very small percentage of all possible breaches that have occurred. While they are the most covered and sensationalised by the media, generally they do not have any material effect on the operations nor do they compromise the integrity of the data (in most cases).

.....

The highest form of risk comes from your own employees and contractors.

RTO Software ensures that our employees and contractors are bound by confidentiality obligations and we also have other items in place such as strong password policies (refer to our data security policy) and other measures to minimise risk from our employees and contractors.

We recommend that you take the following security measures:

a) Ensure that all employees that have access to your confidential data are obligated to sign a confidentiality agreement.

b) Make a rule within the organisation that your access passwords are not shared and kept sure. All passwords should also be a minimum of 12

(twelve) characters in length and be a mix of letters, numbers and special characters. All passwords should also expire on a regular basis (at a minimum every six to twelve weeks if not sooner).

c) As soon as an employee leaves or resigns, all their access accounts should be disabled and their passwords changed. If they have worked closely with any employees it is recommended that the access passwords of those employees should also be changed in the event of a password being shared between employees

d) Any breaches that happen within your organisation should be recorded and kept on file to help build up information that can be used at a review.

e) A security meeting is held on a regular basis between management and staff that highlights any issues that may result in or may cause a breach in security and confidentiality. Any staff concerns should be noted on file and any suspicious behaviour should be brought to attention of the management staff.

.....

What happens in the event of a security breach?

In the unlikely event of a security breach, the following steps are taken depending on the type of breach and its possibility of recurrence.

If the breach was a low risk event and has a minimal chance of recurring, it is noted in RTO Software' internal security logs and recorded. Steps are taken to rectify the cause of that breach and any updates or changes are applied immediately.

In the event of a breach being a medium or a high risk event, we report this breach to the Office of the Australian Information Commissioner (OAIC) and the individuals are also notified immediately.

If necessary the services and applications that are affected are taken offline and steps are taken to remedy the breach. If the steps can be taken successfully and the possibility of a recurrence is minimal, the services and application sites are reinstated. A security breach meeting is

requested between yourself and us to discuss the ramifications of this breach and further action that may be necessary.

In the event of a breach occurring from your side (such as a disgruntled employee gaining access and printing off information), upon notification by you, we take steps to remedy that breach from occurring in the future. A security breach meeting is requested with your organisation to prevent such breaches from occurring in the future.

.....

What are your obligations?

Your obligations are to ensure that all measures are taken to ensure that your staff members and affiliates have suitable access to the applications provided to you by us. Appropriate security permissions setup, strong passwords, confidentiality agreements and other such measures deemed to be reasonable and responsible must be implemented within your organisation.

You are under obligation to inform us of a breach as soon as possible to allow us to remedy it.

You are further obligated to act based on our written recommendations in response to a security threat or a breach or an attempted breach.

Failing to act based on our recommendations or taking the due diligence to ensure that your data is kept safe and only available to appropriate personnel based on security permissions may null and void the obligations of RTO Software and you will be deemed liable for any further breaches.

.....

What are our obligations?

We are obligated to take all necessary steps deemed reasonable to ensure the security and privacy of your data. We do that explicitly in our Data Security and Privacy Policy.

We are obligated to inform you immediately of any medium or high risk security breach. Any low level breaches are recorded in our internal security logs and are made available upon request to any client.

We are obligated to take any and all steps necessary to remedy a breach at the earliest possible time and to undertake steps necessary to minimise the risk of a similar breach occurring in the future.

We are obligated to inform you of any suspicious activity occurring on your application websites such as greatly increased traffic, failed logins and any other suspicious activity that we can track and report on.

We are also obliged to report to the Office of the Australian Information Commissioner (OAIC) about significant data breaches as per the Notifiable Data Breaches (NDB) scheme.

.....

What is the extent of our liability?

Our liability is limited to:

A. Notifying you immediately (upon detection) of any medium to high risk breach,
B. Remedying the breach and taking all steps necessary at our cost to remedy the breach (unless it was a breach caused by your employee / agent in which case charges may be applicable),
C. Taking steps to reduce the possibility of such a breach occurring in the future,
D. In the event that you are not satisfied with any of the above, we can enable stopping the use of the application and its related websites and returning you your data and all related information to allow you to use a different application or business process from another provider / party.

Under no circumstances does RTO Software undertake any financial liability resulting from a breach be it in the form of a loss (real or perceived), business disruption or any other costs associated with the security breach.

Schedule Five

Support Process Statement

Last updated: 7th April 2023

Introduction

The steps we take to deliver efficient and professional support to our clients and to ensure that we are providing a high level of customer service are outlined in this document.

This document outlines the support process for all RTO Software clients.

Contents:

.....

Product Implementation Process

You will be given a 'live' site where you will be setting up all the necessary data and learning how to use the program. At this stage we understand that you will have many questions and the major outcome is to get your site ready for going 'live' and have your staff trained in the application.

RTO Software has a web based Customer Support Centre where our clients have an individual & confidential client site to log any issues and questions which the support team is automatically notified of. Your key staff members will be given user accounts to log into this support centre as well as documentation on how to use the support centre.

The product implementation process is broken into 3 stages that we are committed to completing within the first 30 days of you signing onto one of our products.

These stages include:

Stage 1: Technical & Business Analysis & Stage 1 Product Training

This is where members of our development and support/training teams will need to have access to key staff members from each department of your business.

Our team members will need to collect information pertaining to your business that will allow them to assist you with the setup of your database and where applicable create a data conversion program to convert your existing data into the new database.

The information and database/s that our technical team gathers will help them to create a data conversion program to convert your current data from your existing databases into our product's database. We will need the assistance of your relevant staff members to answer all the questions our technical team have and to also provide guidance as to your business processes & procedures so they can identify any issues with the conversion or how the product will operate for you. This may be a repetitious process but an important one to complete for RTO Software to successfully create a data conversion program.

The information that the support/training staff gathers will allow them to provide you and your staff members with the correct training materials and product training assessment tasks. This stage 1 product training must be completed by your staff within the first 5 days of signing onto the product.

RTO Software has a commitment to complete this section of product implementation within the first 5 days of you signing onto the product.

Stage 2: Product Training and data conversion finalization

This stage is where key staff members from each of your departments will need to complete the products process training and complete relevant assessment tasks for the training. RTO Software support staff will also be available to answer any questions your staff have on the business processes within the product and can assist your staff with their product training assessment tasks.

If needed or it is deemed that a test site is applicable, you will be given a 2nd product site and the technical team will convert your data into this site. Your key staff members' will then need to test the data in this site and will need to give final approval of the conversion program at this stage ready for the final conversion of data for your live site. This process may also be repetitious to complete a final/approved data conversion program.

RTO Software has a commitment to complete this section of product implementation within the first 20 (twenty) working days of you signing onto the product. Please note that your full cooperation in procurement, cleaning and quality checking of data is needed to achieve the above deadlines.

Stage 3: Final Data Conversion/Go Live Process

This is where your key staff members from each department must have completed their product training and also delivered product training to nonkey members within their department prior to going 'live' with your product.

Also at this stage of product implementation RTO Software takes a final copy of your current database/s and runs the approved data conversion into your live product site. The final data conversion is generally completed over a weekend ready for you to go live on the following Monday.

The final step is for you to go live on the Monday morning with your new product.

RTO Software has a commitment to complete this section of product implementation within 30 days of your signing onto the product.

The first week that you go 'live' with the product a RTO Software will be available to your staff to answer questions or assist you with any issues you may have.

.....

Ongoing Support Process

As part of our commitment to providing efficient, professional and quality customer support all clients are given user accounts to our Customer Support Centre. Here you will be able to log issues, questions and product improvements/suggestions. Once they are logged they become an 'Action' and are allocated a unique ID #. The support team is notified of these 'Actions' immediately. From there the actions are prioritized into the following categories:

Critical (an issue that stops you from using TEAMS or a process within TEAMS completely, there is no work around at all) **fixed immediately within 4 (four) hours** – you MUST contact RTO Software support staff on our support line which is 1300 850 585.

High (an issue that stops you from using a process in TEAMS but there is a workaround) **within 48 (forty eight) hours the issue will be fixed** – you MUST log these issues in the Customer Support Area.

Medium (an issue that is not stopping you from using TEAMS but is not an improvement or suggestion) within 5 (five) working days the issue will be fixed – you MUST log these issue in the Customer Support Area.

Low (an improvement or suggestion changes for TEAMS but it is not stopping you from using TEAMS) – will be scheduled for the next version update – you MUST log these issues in the Customer Support Area.

As part of our ongoing support process from the moment a client is live the following process is also implemented:

1st month after going live – RTO Software support staff will contact your product representative/s once per week to check on how everything is going and answer any questions you may have or help you to rectify any issues you may have.

2nd month after going live – RTO Software support staff will contact your product representative/s once per fortnight to check how everything is going and answer any questions you may have or help you to rectify any issues you may have.

3rd month & onwards after going live RTO Software support staff will contact your product representative/s once per month to check how everything is going and answer any questions you may have or help you to rectify any issues you may have.

.....

Support Initiatives:

As part of our ongoing support process and evaluation we also have the following support initiatives in place:

Intermittent questionnaires for us to evaluate the product implementation and support processes.

Six monthly & yearly product implementation review to evaluate how you are using the product and are there any further training requirements or do you wish to use other areas of the product that you may not have chosen to use when first implemented.

Intermittent surveys that allow us to understand any further support or product development requirements.

http://www.rtosoftware.com.au is a site for our clients to use along with support@rtosoftware.com.au to email and discuss issues relating to their use of TEAMS and its related items. You can also create articles to post in the User Forums and it is also a place where you can post new development items you would like to see in future releases of your product.

Product Future Development Client Forums – the products we build are for you and your business. We believe that the most important part of a product is its ability to grow as your business and the industry grows. With our products they support large areas of specific industries so not all

users will use all areas of product. We ask our clients who have an invested interest in specific areas of a product continuing to grow as they grow to become members of specific product client forums. These forums allow our clients to discuss the future growth and development of the product and specific areas of the product as well.

RTO Software believes in agile development with constant and never ending improvements and we are always looking to improve our products and support processes and are open to suggestions and ideas from our clients.

.....

Review of this policy:

If there are any material changes to this policy affecting your rights as outlined above, you will be notified of the change. This policy is available for viewing on our website and is also made available to any third party auditors or security auditors upon request.

Schedule Six

Data Release Policy

Last updated: 26th January 2024

Introduction

We appreciate that there are regulatory authorities that have an interest in the data held with us in the unlikely event of you ceasing to operate or being placed under receivership due to financial or other reasons or the students being no longer supported by you. This poses a risk and may obligate a government body to intervene and contact us for release of important student related data for enabling further placement.

This document sets out our policies relating to the steps we undertake in the unlikely event of this occurring. This policy document should be read in conjunction with the Software Licence Agreement (if applicable).

Contents

.....

What happens if the client cannot continue its operations?

In the unlikely event of a client going bankrupt, financially in receivership or for any other reason is unable to provide services to your students, we will continue to support the application designed by us and release related student data to applicable government authorities (upon their request); we have this data release policy.

RTO Software has a data backup policy that ensures that client data is regularly backed up and able to be restored as needed. In the event that you do not or cannot provide services to the students any longer, we will release to the applicable governing body (in your state or territory) a set of files to allow them to access your student data including the name and other bio and demographic details of students, details of the courses they were enrolled in, student progress and results obtained and any other critical information required by law or regulation to allow the successful future placement of the affected students.

.....

Who has the right to contact us and how?

RTO Software can be initially contacted via phone on 1300 85 05 85 to inform us of the change in status with the client. This contact can only be made by an authorised and nominated representative from the client or an authorised representative of the appropriate government regulatory body.

Furthermore, a written confirmation will need to be sent either by email or by post. The written confirmation will need to be sent by email to either support@rtosoftware.com.au or by post to PO Box 7511, Gold

Coast MC, QLD 4209. We will endeavour to respond to your request within seven days.

The nominated person that can be contacted with regards to this is Ms Melissa Hamilton-Matthews. She can also be directly reached via email on melissa@rtosoftware.com.au.

We will try to contact the client and verify that they are indeed no longer servicing the students (if possible). If we are unable to contact the client or it is released as public knowledge (verified media release etc) that the client is no longer in operation, this will be deemed as sufficient and reasonable cause to release the data only to the appropriate government body upon request.

.....

What will we do with the student data?

All our Client's databases are regularly backed up and protected. We will export the relevant student data into (one or many) CSV files and make them available to the regulatory body as per this policy. This service will be provided at a nominal charge.

.....

What are the client's / governing body's rights?

You rights are:

- To install a copy of this released data as per the instructions to a local PC or server.

- To use this data without payment of any fees or charges for as long as you wish to use it.

- To copy this data as long as it is for your organisation’s or governing body's use only.

.....

What are the client's / governing body's obligations?

The data release policy is designed to safeguard the public interest in the event of the client unable to provide the students continued services.

While the governing body has the rights to obtain a copy of the student data for use on their local PCs or local servers, the released data must not be:

- Copied or resold to any third parties that are not involved in the student placement process.
- Modified or otherwise alter the originally released data in any way. Originals must be kept as is.
- Used to claim any rights over the data apart from the right to use it.
- used to profit from the data either directly or indirectly in any form.

Schedule Seven

Cyber Security Policy

Last updated: 26th February 2024

Introduction

Our primary purpose of the Cybersecurity Policy is to establish and maintain a secure digital environment to protect the integrity, confidentiality, and availability of our information and systems. This policy provides the framework for protecting our SaaS platform against potential cybersecurity threats and risks, ensuring that we continue to meet the trust expectations of our clients and comply with applicable legal and regulatory requirements in the VET sector. Our commitment is to safeguard sensitive data related to students, educational institutions, and our operational processes from unauthorised access, use, disruption, modification, or destruction.

This policy applies to all employees, contractors, and third-party service providers of RTO Software, encompassing all organizational operations involving data processing, information systems, and communication technologies. The scope includes, but is not limited to:

Contents

.....

Data Protection and Privacy:

We are committed to safeguarding personal and financial information in compliance with Australian Privacy Principles. We collect necessary data solely for delivering our SaaS services, informing students about usage. Data is protected with robust encryption and accessed only by authorized personnel. We retain information only as required and ensure secure disposal. All staff receive training on privacy protocols. We conduct annual reviews and enforce compliance strictly, addressing any breaches with appropriate actions. This ensures transparency and trust in our handling of sensitive data.

.....

Access Control:

We implement stringent access controls to protect sensitive data within our SaaS platforms. Access to information is granted based on job roles and the principle of least privilege, ensuring that individuals receive only the access necessary for their duties. We employ multi-factor authentication and periodic access reviews to maintain security integrity. Access logs are monitored continuously to detect unauthorised attempts and ensure compliance. These measures are critical in preventing data breaches and maintaining the trust of our clients in the vocational education sector.

.....

Incident Response and Management:

We have established a robust incident response plan to swiftly address and mitigate cybersecurity threats. Our dedicated Incident Response Team is trained to act immediately upon detection of a security breach. The procedure includes identifying the scope of the incident, containing the breach, and swiftly recovering systems. We communicate openly with all affected parties and comply with legal reporting requirements. Continuous improvement through lessons learned and feedback ensures our response strategies evolve with emerging cyber threats, maintaining the security and integrity of our services.

.....

Network Security:

At RTO Software, we uphold stringent network security protocols to safeguard the integrity and confidentiality of data. Our security infrastructure includes advanced firewalls, intrusion detection systems, and encrypted VPN connections for secure data exchanges. We implement high-standard encryption for data at rest and in transit to fortify our defences against cyber threats. Continuous security audits and proactive network traffic monitoring are integral to our strategy, enabling swift threat detection and response. These rigorous measures ensure the protection of our vocational college clients' sensitive information, reinforcing the reliability and security of our applications.

.....

Regular Audits and Compliance Checks:

RTO Software is dedicated to upholding the highest standards of cybersecurity through systematic audits and rigorous compliance checks. We engage in bi-annual independent assessments to scrutinize our security protocols, pinpoint vulnerabilities, and confirm compliance with industry and regulatory norms. Our partnerships with external cybersecurity specialists guarantee an objective evaluation of our systems and procedures.

Our dedicated compliance team actively tracks and adapts to changing regulations to ensure we meet all applicable cybersecurity standards. Any issues discovered during audits are swiftly rectified to fortify our security framework.

This proactive regimen not only ensures consistent compliance but also strengthens our dedication to safeguarding our clients' data.

.....

Employee Training and Awareness:

At RTO Software, we emphasise Employee Training and Awareness as a vital pillar of our cybersecurity strategy, incorporating several key initiatives:

- Initial Security Orientation: Any new employee undergoes compulsory training to understand our security protocols and their individual security responsibilities.
- Annual Refresher Training: We ensure all staff members receive updates on the latest cybersecurity practices and regulatory

obligations to maintain high compliance and awareness levels.

- Targeted Expert Workshops: We regularly host expert-led sessions that delve into current and emerging cybersecurity threats, enhancing our team's ability to identify and mitigate potential risks.

- Practical Security Exercises: Through interactive simulations, such as simulated attacks, we actively engage our staff in realistic scenarios to strengthen their hands-on security skills.

This structured approach not only maintains high standards of compliance but also cultivates a proactive security culture within our team, ultimately protecting the sensitive information of our clients in the vocational education sector.

.....

Physical Security:

RTO Software vigorously enforces robust physical security measures to safeguard our premises and the critical data within. Our physical security framework includes:

- Controlled Access: Access to our server facilities are strictly regulated. This includes using state-of-the-art biometric and electronic access control systems, ensuring that only authorised personnel can enter.

- Surveillance: Our server premises are monitored around the clock with comprehensive CCTV systems, providing real-time security oversight and incident response.

- Visitor Management: A stringent visitor policy that requires all guests to sign in, show identification, and be escorted at all times within secure zones.

- Environmental Protections: Advanced fire suppression and climate control systems are deployed to protect against environmental risks and ensure operational continuity.

These proactive physical security protocols are crucial for protecting our operational infrastructure and the confidential data of the vocational education providers we serve.

.....

Third-Party Vendor Management:

We employ a stringent Third-Party Vendor Management strategy to ensure the security and integrity of our services:

- **Vendor Selection:** We conduct thorough security assessments before entering agreements to ensure vendors meet our high standards.
- **Contractual Requirements:** Contracts mandate strict adherence to our security protocols and data management practices.
- **Ongoing Oversight:** We routinely audit vendor compliance to confirm continuous adherence to our standards.
- **Risk Mitigation:** Vendors are evaluated and managed based on the specific risks they present to our operations.

.....

Risk Assessment and Management:

We prioritize a proactive approach to risk assessment and management, focusing on preserving the security and integrity of our services. We consistently identify and evaluate risks inherent in our operational processes and employ effective measures to mitigate these risks. Key initiatives include regular updates to our security protocols, continuous enhancement of employee training programs, and fortification of our technological infrastructures.

Our risk management team utilises a range of tools and techniques to continuously monitor and respond to emerging threats, ensuring our ability to adapt quickly to the evolving cybersecurity environment. This strategic focus is essential for protecting the sensitive data of the vocational education sector and maintaining the confidence of our clients.

.....

Policy Review and Update Procedures:

RTO Software is dedicated to maintaining up-to-date and effective cybersecurity policies through a systematic review and update process:

Annual Reviews: Our policies are reviewed at least annually or in response to significant changes in technology, legal requirements, or operational shifts.

Cross-functional Collaboration: The review process is collaborative, involving inputs from cybersecurity experts, legal advisors, and operational leaders to ensure comprehensive policy coverage.

Incorporating Feedback: We integrate feedback from internal audits, employee suggestions, and external assessments to refine our policies.

Updating Procedures: Any necessary updates are rapidly implemented to address new security challenges and regulatory demands.

Employee Communication: Updated policies are disseminated through mandatory training sessions and internal communications to ensure company-wide compliance and understanding.

This structured approach ensures that our cybersecurity measures remain robust and responsive to the evolving threat landscape, safeguarding the sensitive information of our clients.