



Welcome to TRC

Awareness Guide for Information Technology

PLEASE READ THROUGH THIS DOCUMENT IN ITS ENTIRETY. THERE IS IMPORTANT POLICY AND SUPPORT INFORMATION AS WELL AS REGISTRATION INSTRUCTIONS FOR YOU TO COMPLETE AS YOU GET STARTED USING THE TRC'S INFORMATION TECHNOLOGY ENVIRONMENT.

May 31, 2016

Table of Contents

1. [Logging In](#)
2. [Password Self-service](#)
3. [Office 365](#)
4. [Collaboration](#)
5. [Internet Usage](#)
6. [Remote Access](#)
7. [Wireless](#)
8. [IT Support](#)
9. [IT Procurement](#)
10. [Maintenance Windows](#)

Logging In

User Account – All TRC employees have a user account for logging into the network. You will be given your ID by your manager in most cases with a one-time use password that must be changed at first log in. All employee user accounts are part of the “Employees” domain. When prompted to authenticate with the network, you will be required to supply your User ID (not case sensitive), your password (case sensitive) and the Domain to which you are logging in. (example – employees\username).

Password Policy - All user-chosen passwords must meet the following criteria:

- Must be a minimum of 8 characters in length.
- Must contain 3 out of 4 types of characters: Uppercase, Lowercase, Numbers, and Special Symbols.
- Cannot contain your User Id or Full Name
- Must be different from the 4 previous passwords

Password Expiration:

- Must be changed every 90 days

Password recommendations:

All passwords should be difficult for someone else to guess. They should not include simple letter or numeric sequences. It needs to be difficult to guess. Words in a dictionary regardless of language, derivatives of user-IDs, and common character sequences, such as "123456" are not permissible. Likewise, personal details such as spouse's name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords must also not be part of common speech regardless of language. For example, proper names, geographical locations, common acronyms, and slang must not be employed.

Users are prohibited from constructing passwords made up of a fixed number of characters that do not change combined with a fixed number of characters which predictably change. In these prohibited passwords, changed characters are typically based on the month, a department, a project, or some other easily guessed factor. For example, users must not employ passwords like "A12JAN" in January, "A12FEB" in February, etc.

Password Lockout Policy:

After 10 invalid attempts the password is locked out for 20 minutes.

Password Sharing:

Passwords are NOT to be shared. All users are responsible for actions performed under their User ID.

For the complete Password Policy Documentation, please see IT3-8 Password Construction Guideline and IT3-8 Password Protection Policy located under Policies -> IT on TRCNET (<http://trcnet.trcsolutions.com>).

Password Policy for Vision

Vision Users are authenticated into the application based upon their TRC User ID and Password

Enforcement:

Any employee or third party found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

15 Minute Desktop Lockout:

After 15 minutes of inactivity, your desktop / laptop screen will lock requiring you to enter your credentials to access the system again.

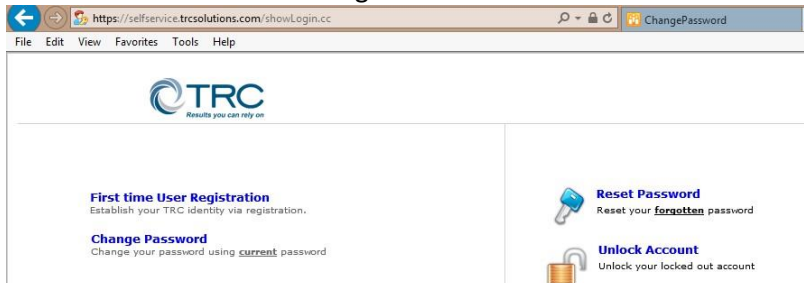
Desktop Authority / Scripting:

When logging into the network – before actually reaching the desktop – Desktop Authority will run on your system every time you log in. It will also run when you log out. Desktop Authority is used to push out Drive Mappings, Printer shares and a host of other options that TRC uses to optimize the user experience within the network. If you experience problems with Desktop Authority, please submit an IT General Service Request through the ServiceDesk (See Section 8).

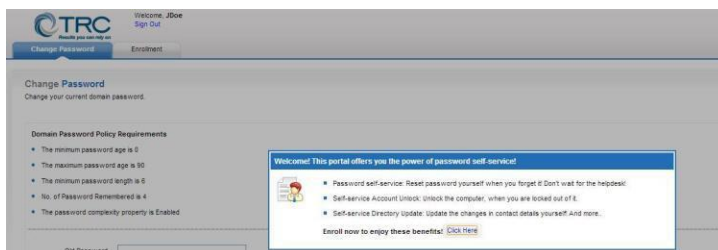
Self-Service password maintenance - required

Steps to complete one time registration

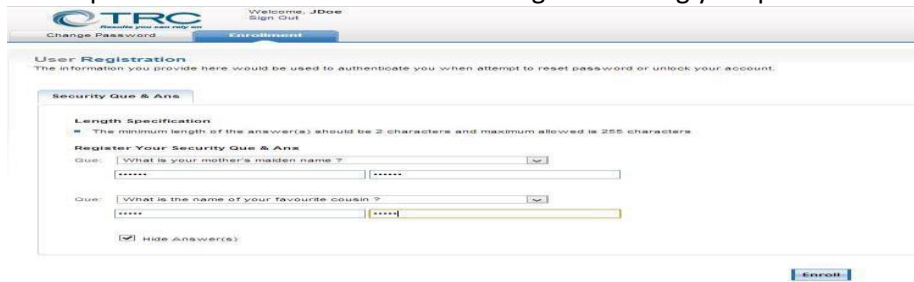
1. <https://selfservice.trcsolutions.com> (available both inside and outside TRC network).
2. Select “First time User Registration”



3. Login using your TRC network ID and password
4. Clicking on the “Click Here” link.



5. Select and complete two of the available questions. You will be prompted for the answers to the questions in the future when unlocking or resetting your password.



6. You will see a successful enrollment message from the portal, at this time your one time registration is completed and you can close the page.

Self-service Password Reset or unlock usage

When your password needs to be reset or unlocked you can access the site via:

1. <https://selfservice.trcsolutions.com>
2. Using the Self-Service Password app on your mobile phone.
 - a. For iOS, the app is named: **ADSelfService Plus** from Manage Engine, available in Apple App Store or TRC App Catalog
 - b. For Android, the app is also named: **ADSelfService Plus** from Manage Engine, available in Google Play Store

For complete documentation on the Self Service Reset tool, please see IT3-8 Self Service Account Management and IT3-8 SOP Self Service Registration and Use under Policies -> IT on TRCNET (<http://trcnet.trcsolutions.com>)

Microsoft Office 365

TRC uses Microsoft's Office 365 suite of applications including Word, Excel, PowerPoint, Outlook, OneNote, Skype for Business, and OneDrive for Business. These apps are all cloud-based but also include locally installed applications.

Skype for Business

- Instant Messaging – Real-Time communication internally with other TRC users of Skype for Business.
- Audio and Video meeting & conferencing
 - Modern meetings with powerful collaboration features
 - Integrates with Outlook Calendar
 - Internal and external participants supported
 - A dial-in integrated conferencing line option via Intercall is available by request

OneDrive for Business – Your TRC Cloud Storage

- Securely store up to 1 TB of data which is synchronized and/or accessible on all of your corporate devices including mobile
- Easily share folders or files with colleagues or external parties
- Live collaboration on Office documents using Office Online
- Fully integrated with Microsoft Office and Office 365

Rights Management – Persistent security and access controls for sensitive data

Rights Management is a platform and framework which is built into Microsoft Office and Office 365 that allows you to apply persistent protection and access controls to documents containing sensitive data. You can easily share documents with colleagues and trusted third parties while maintaining control over the data. The following are a few examples of some of the things you can do with Rights Management platform:

- Safely share project documents with a client via email
- Send data containing personal customer information over email to a team member in the field
- Protect company-confidential spreadsheets stored on your laptop, network file share or OneDrive

Email (Outlook)

- **Mailbox Size Limits** – 50 GB Primary Storage; 100 GB Archive
- **Message Size (Attachment Limits)** – The maximum size for an individual message including attachments is 25 MB, both incoming and outgoing. NOTE: Other organizations may set different limits. When possible, avoid sending attachments and share via AdHocFTP (See File Transfers: external below) or OneDrive for Business.
- **Recipient Limits** – The maximum number of recipients for a single message is 500 (an internal distribution list counts as one recipient). For help or questions, contact TRC IT ServiceDesk.

Remote Email Access

In addition to having access to your e-mail through Outlook on your computer and your smartphone, you can access your e-mail via:

- TRCNet.trcsolutions.com: Select **Office 365 Portal** on the left side of the TRCNet Home page
- Direct URL: outlook.com/trcsolutions.com (Enter your TRC email address and password)

Spam and Virus Protection

Office 365 Exchange Online Protection (EOP) will scan all incoming and outgoing messages for spam, viruses, and malware. EOP spam filtering works in part by assigning a spam confidence level (SCL) based on the likelihood that a message is spam. Depending on the SCL, an inbound message may be relayed directly to your Junk Email folder in Outlook, or blocked outright at the server. Messages detected as containing viruses and malware are stopped at the server. You should never see these messages in your Junk Email folder or Inbox. If you suspect that a message with malicious content or attachments in your mailbox, please avoid opening the message or attachments, and forward the message to IT ServiceDesk.

Junk Email Folder

Spammers are always looking for new ways around filters, and EOP does a good job of keeping up with these evolving threats. However, there is a chance you will occasionally receive legitimate email in your Junk Email folder in Outlook. Conversely, you may occasionally receive what appears to be spam in your Inbox. Outlook makes it easy to tag these senders or domains as junk or not junk by adding them to a personal safe senders and blocked senders lists. Right-click on a message in Outlook and select either 'Block sender' or 'Never block sender.'

You may also submit the messages to Microsoft EOP team for review and inclusion in their filtering engines. To do so, forward the message as an attachment to the corresponding email address, Junk@office365.microsoft.com or Not_Junk@office365.microsoft.com.

Forward a message as an attachment:

Begin a new message, then copy and paste the desired message into the new message or select the message, choose **More > Forward as attachment** on the Home ribbon under the Respond section.

Email for Personal Devices

TRC provides support for email synchronization on personal devices provided that they are registered with TRC's MDM application, Intune. People wishing to synchronize mail to their personal devices may seek assistance through the Service Desk.

NOTE: TRC IT Personnel will support personal devices only on a Best Effort basis.

Collaboration

SharePoint / TRCNet – TRC is currently utilizing SharePoint as its primary Collaboration platform; both within TRC and with externally with clients & vendors. Communities can be established for Projects. Both Clients & Vendors may be given external ID's with which to access said communities. Please open a SharePoint Ticket on the Service Desk to request the creation of project communities or the granting of permissions to Clients or Vendors.

- **How to login to TRCNET:** <http://trcnet.trcsolutions.com/>

- **TRC Employees:**

- *Inside TRC network (including VPN)*

- Internet Explorer you will not be prompted for username or password.
 - Other Browsers you will be prompted with the screen below:
 - Please select TRC Employee and enter your TRC ID and Password



- *Outside TRC network (All Browsers)*

- Login from non-TRC device or TRC computer not connected via VPN, you will be presented with the screen above. Please select TRC Employee and enter your network username and password.

- **Non TRC employees:**

- *Public Internet*

- When logging in from public internet, Non TRC Employees will be presented with the screen above. External user option should be selected along with a username and password.
 - *Existing* external users will use the existing username. A new password will be emailed directly and shared with the "Portal" community leaders as well.

- New external users will be able to create username and password of their choice by clicking on the link that will be provided by the community leaders.

Internet Usage

Web Access

Internet access is available to all TRC employees within TRC office locations.

Web Content Filtering

TRC employs a filtering service that restricts access to certain websites. Access restrictions are set by the provider. The block list is updated on a regular basis using a restriction set by a global organization. In addition to the block list, the site content is scanned by an antivirus engine and certificate authority before the content is delivered to your browser to certify the identity of the website. If a site does not pass all restrictions a Websense Blocking Page notification will appear in your browser screen. The blocking page will list the reason the page was blocked as well as the exact URL that was blocked.

Quota Time

All websites classified as File Storage or Personal Backup are blocked by default, but can be accessed by using "Quota Time". TRC allows for four 15-minute sessions daily to access such sites.

If a site is "Quota Time" enabled there will be a "Use Quota Time" button at the center of the Websense blocking page.

Access

Click on the "Use Quota Time" button to be passed through to the website. If you are transferring a file that cannot be transferred in 15 minutes, the transfer WILL continue even if your current 15 minute session expires. NOTE: If you are accessing a website using HTTPS there will NOT be a Websense blocking page. Try accessing the page via HTTP instead to access the Quota Time button.

Unblocking a website

There are times that websites become mistakenly categorized by Websense as restricted. You may also need access to a website that is normally blocked by policy. To request access to a blocked site open an IT General Request, select category "Other" (using the ServiceDesk website), include a screen shot of the Websense blocking page and the business reason you need access.

Exceptions

If a website shows that it has been blocked as 'Malicious', this is usually indicated if there is code on the website that can be used to infect or otherwise harm systems accessing it. By policy, those websites will not be unblocked. You can however, submit a request to unblock the website and a request will be sent to Websense to evaluate the site in question to determine if the threat status of the website is considered current.

File Transfers

Internal:

TRC has an internal only FTP site at FTP.TRCSolutions.com. If you need to store data there please submit a Service Request for assistance. Please Note: The FTP Site is NOT backed up. It is not intended for long term storage.

External:

Transferring large files to users outside of TRC can be accomplished using our Ad hoc File Transfer feature within TRCNet. <https://adhocftp.trcsolutions.com/AHT/> (This link is accessible from the right hand side of the TRCNet homepage.

- Login information required:
 - Username - username@trcsolutions.com
 - Password - TRC network password.

Remote Network Connectivity via VPN

- TRC Personnel may connect to the network using the installed and configured Cisco VPN client on a TRC imaged system.
- Connecting via Cisco VPN client:
- Start the Cisco VPN software
- Select and click the TRC Network entry
- You will be prompted for your TRC network ID (employees\JSmith) and Password.

Wireless

Offices are equipped with three wireless networks namely TRC, TRCMOBILE and TRCGuest.

- TRC (Employee Only): will allow for the access to the corporate network. This connection may only be used by corporate devices. (Enter Network Credentials when prompted)
- TRCMOBILE (Employee Only): this device allows for internet access only. This connection may only be used by employee owned devices (BYOD)
- TRCGuest (for Visitors): allocated bandwidth is 1 MB. This connection may only be used by TRC Guests / Clients for Internet access.
 - Prompts for authentication “similar to screenshot below”, credentials are provided to the office manager/admin at each location.



Powered by www.vivacomm.com © 2004-2009

IT Support

ServiceDesk

Service requests for IT support should be submitted through TRC's ServiceDesk at [HTTP://ServiceDesk.TRCSolutions.com](http://ServiceDesk.TRCSolutions.com). This site is accessible both internally and externally. You can also access the site using a smartphone by accessing [HTTP://ServiceDesk.TRCSolutions.com/mobile](http://ServiceDesk.TRCSolutions.com/mobile).

Alternate options for Service Request:

- Call 1-866-644-4TRC Select Option 0 to speak with a Support Specialist who will open a service request for you.
 - Available 24X7; non-urgent requests will be addressed next business day
- Email: ITServiceDesk@TRCSolutions.com

You will receive an emailed notification once the ticket is opened. Future email communications related to this incident or request should be in response to one of the system notifications for this ticket. This will update the original ticket.

Ticket status checks or edits can be performed by visiting the My ServiceDesk Incident or My ServiceDesk Requests on the ServiceDesk website or mobile site.

On Demand Expert Assistance on "How To" questions for Microsoft Office including Skype and CRM, Adobe Suite including Acrobat, and more.

- Call 1-855-230-8227 (available 24x7)

IT Procurement

All software and hardware must be purchased through the IT procurement section of the TRC ServiceDesk home page <http://servicedesk.trcsolutions.com> under the "Order Something" option or via the IT Procurement link on TRCNET.

Maintenance Windows

TRC has a defined Maintenance window of Midnight through 6:00 am ET weekly on Saturdays. Maintenance for enterprise level systems such as Exchange or Vision may be performed and these systems may not be available during this time frame. Advanced notice may be given but is not required. In the event extended maintenance is required outside of this time frame, the outage will be announced via e-mail.