RxLogix Corporation

Anti-Fraud Training

RX-TRN-DevOps-001, Version 1.0

RxLogix

Revision History

Version	Author	Revision Notes	Date
1.0	Sanjeeb Chowdhury	Initial	14-Aug-2020

Fraud prevention

Agenda of this training:

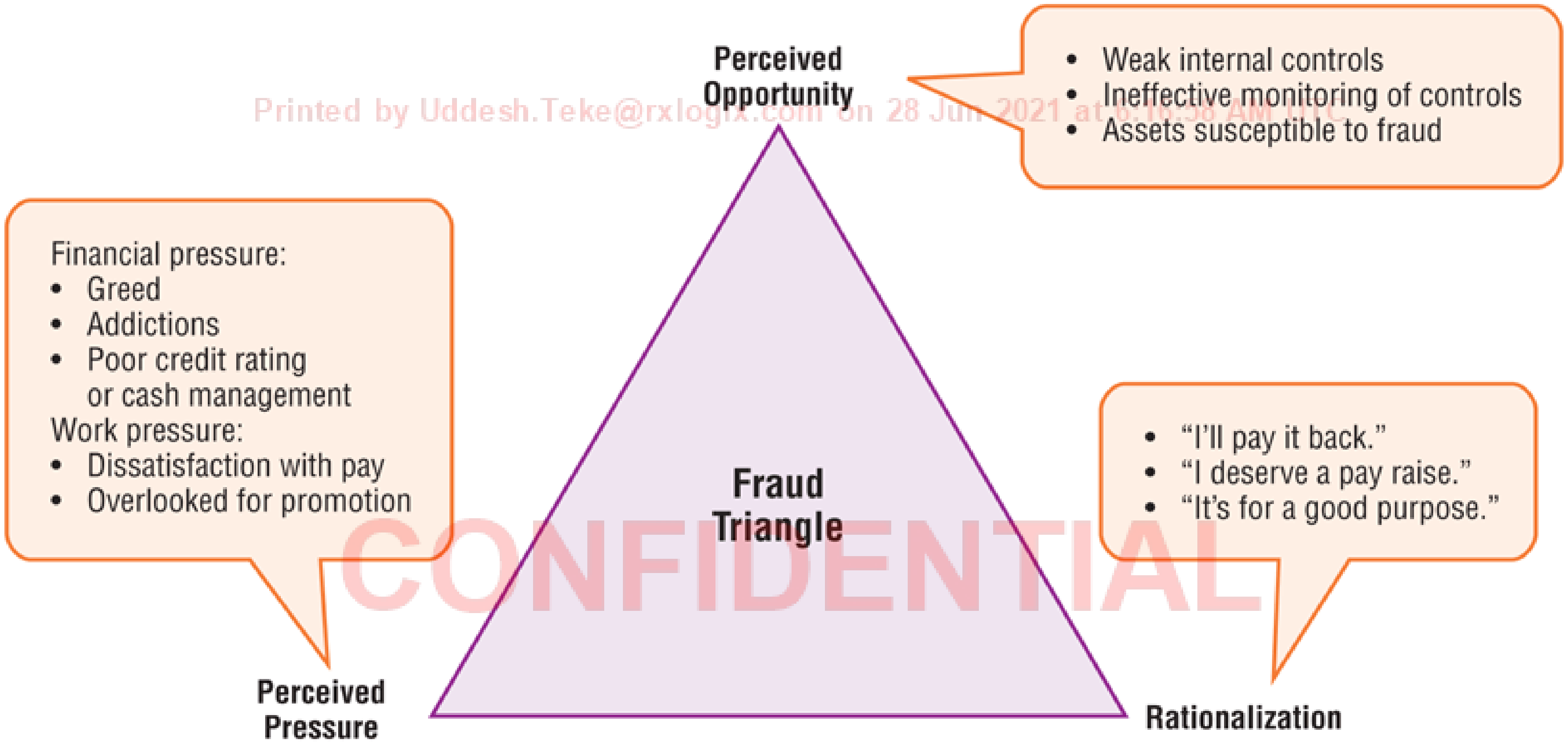
1. What is **Fraud**
2. How fraudster approach for **Fraud**
3. How to prevent **Fraud**
4. Best Practice points for Information security
5. Where to report **Fraud**
6. Questions and Answers

What is Fraud ?

Wrongful or criminal deception intended to result in financial or personal gain

Oxford Dictionary

Why Fraud ?



Perceived Opportunity

- Weak internal controls
- Ineffective monitoring of controls
- Assets susceptible to fraud

Perceived Pressure

Financial pressure:

- Greed
- Addictions
- Poor credit rating or cash management

Work pressure:

- Dissatisfaction with pay
- Overlooked for promotion

Rationalization

- “I’ll pay it back.”
- “I deserve a pay raise.”
- “It’s for a good purpose.”

How fraudster approach for **Fraud**

1. Phishing
2. Vishing
3. Smishing
4. Lottery or Prize claim
5. Tech support
6. Fake refund (Tax or e-com. portal)
7. Cryptocurrency investment schemes

1) Phishing

- Phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords, Bank account and credit card details by fake URL link in e-mail.

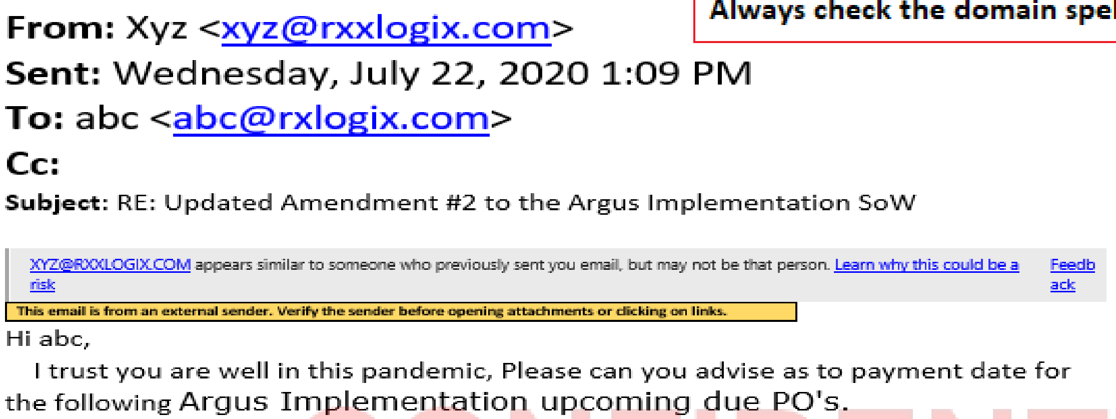
- Phishing can also involve sending malicious attachments or website links that may contain malware or payload with these they can infect computers or mobile devices and get remote access of your devices.

- Phishing e-mail may request to transfer funds into bank account for any fake invoice, fees, rental amount or subscription charges for any services.

Example of Phishing e-mails – looks like similar domain

- Phishing mail may look with similar name and very little difference in the spelling of email id, Example:

Always check the domain spelling of sender



From: Xyz <xyz@rxxlogix.com>
Sent: Wednesday, July 22, 2020 1:09 PM
To: abc <abc@rxlogix.com>
Cc:
Subject: RE: Updated Amendment #2 to the Argus Implementation SoW

XYZ@RXXLOGIX.COM appears similar to someone who previously sent you email, but may not be that person. Learn why this could be a risk

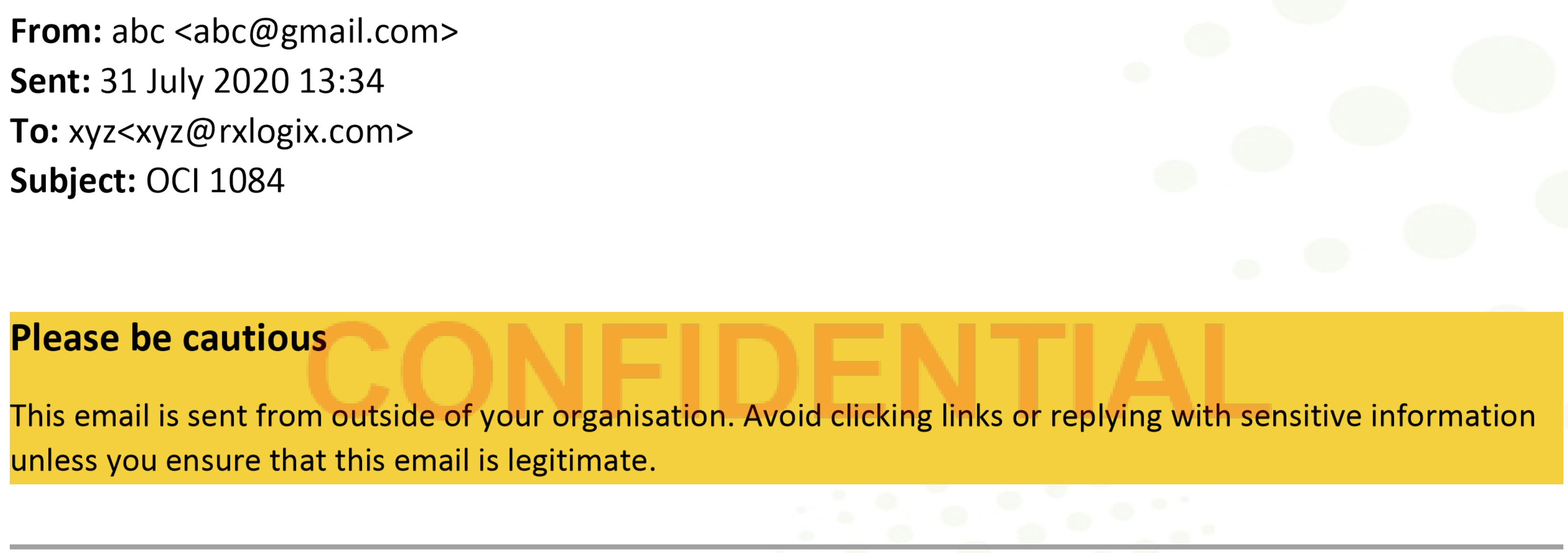
This email is from an external sender. Verify the sender before opening attachments or clicking on links.

Hi abc,

I trust you are well in this pandemic, Please can you advise as to payment date for the following Argus Implementation upcoming due PO's.

Example of Phishing e-mails – **out side e-mail highlighted**

- Be careful, if you received any e-mail from the outside domain of Rxlogix.
- **Out side e-mails will be highlighted in Orange strip, e.g.**



From: abc <abc@gmail.com>
Sent: 31 July 2020 13:34
To: xyz<xyz@rxlogix.com>
Subject: OCI 1084

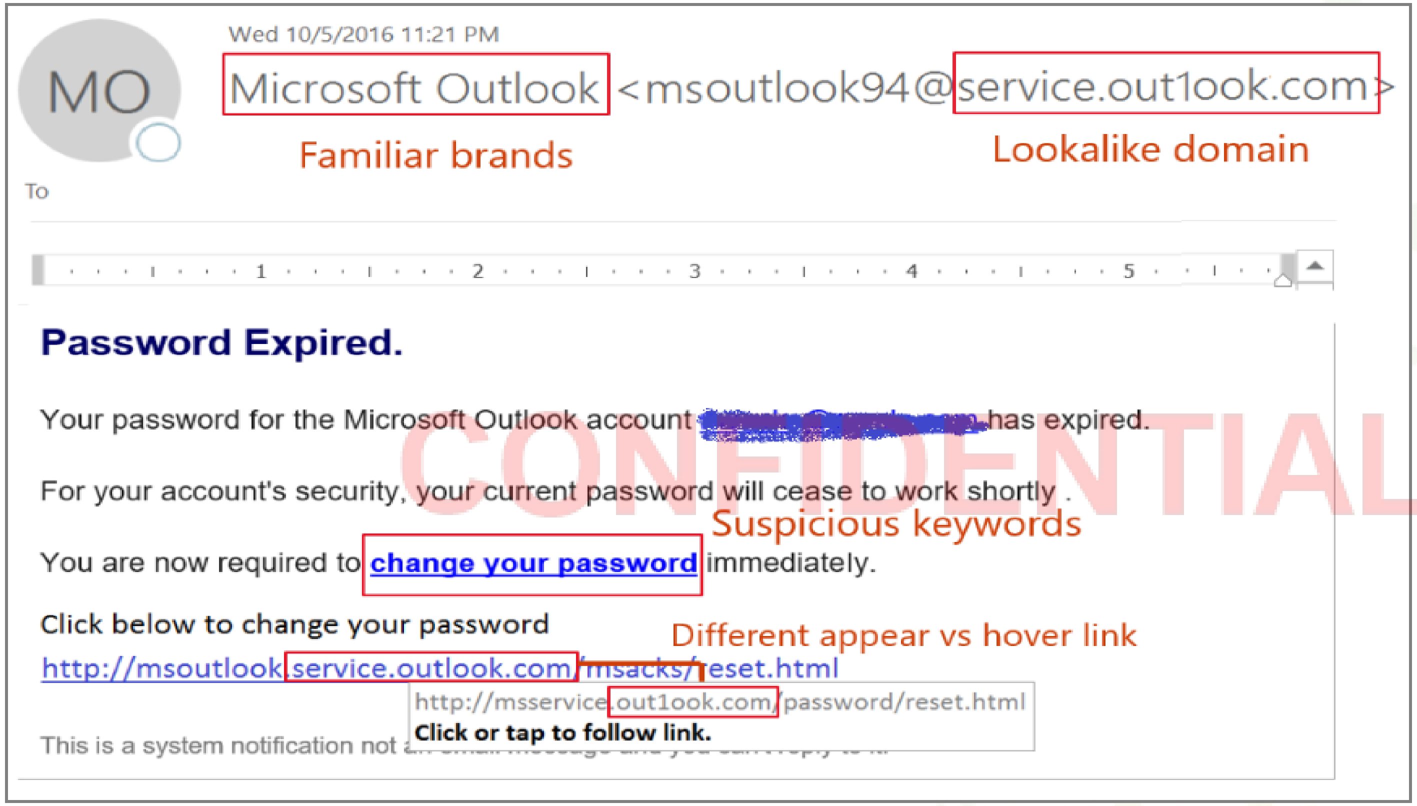
Please be cautious

This email is sent from outside of your organisation. Avoid clicking links or replying with sensitive information unless you ensure that this email is legitimate.

so verify the sender before opening the email

Example of Phishing e-mails– **Password expiry**

Fraudster may send password expiry phishing email with similar domain name, please check the e-mail address from which mail is coming and contact with IT support first if any assistance is required.



Wed 10/5/2016 11:21 PM

Microsoft Outlook <msoutlook94@service.out1ook.com>

To

Password Expired.

Your password for the Microsoft Outlook account [redacted] has expired.

For your account's security, your current password will cease to work shortly .

You are now required to change your password immediately.

Click below to change your password

http://msoutlook.service.outlook.com/msacks/reset.html

http://msservice.out1ook.com/password/reset.html

Click or tap to follow link.

This is a system notification not an email message and you can't reply to it.

2) Vishing (Voice Phishing)

- Vishing is when fraudsters obtain personal details of a victim by phone call

- Bank fraud vishing scams are some of the most common you’ll come across. Scammers will typically pose as a financial institution representative and obtain your bank account and card details eg your card going to expire, bank account going to freeze, KYC not updated then they request to share OTP, password.

- Calls in general are far less abundant than email, so there is a higher chance of getting someone’s attention.

3) Smishing (SMS Scam)

- Smishing is when fraudsters obtain personal details of a victim by SMS text messages.

- In an SMS phishing, or “smishing” attack, targets receive a text message that uses a short code. Often, these messages mimic the legitimate ones you might get, e.g., “Free reward points” confirm your bank transaction.” This type of message would include a shortened link.

- Clicking on shortened link lead to a malicious app being installed on your smartphone. Once it’s on there, the malicious app could track your keystrokes, steal your identity, or encrypt the files on your phone and hold them for ransomware.

4) Lottery or Prize claim

- you get an email that tells you that you have won the lottery/Prize and can claim a huge amount of money, right after you pay a small fee.

- They will ask your all personal information and bank account details and request to send some processing fess to get funds into your account.

5) Tech support Scam

- This scam isn’t always initiated over the phone and might start via a web page popup that tells you your computer is infected and to call a support number.

- A “technician,” claiming to represent a large firm like Microsoft, will tell you your computer is infected, and you need to hand over remote support.

- Once you do, the fake tech executive can do whatever they want with your system, including installing malware or ransomware. Typically, once they are finished “fixing the issue,” you’ll be asked to pay for the service.

6) Fake refund (Tax or e-commerce portal)

- This one targets people who are expecting a tax refund or recent online purchase items from e-commerce website.

- criminals pose as the Income Tax Dept. or similar agency and prompt targets to click a link through which they can claim their refund. However, the link leads to a phishing site where the victim is asked to provide personal information such as their social security number and banking details, which can be used in identity theft.

7) Cryptocurrency investment schemes

- With the cryptocurrency market being so volatile, it’s not uncommon to hear about massive gains over a short period of time.

- Austrian investment scheme Optioment promised a whopping 4% weekly return to some investors and ended up reportedly stealing more than 12,000 bitcoins.

How to prevent Internet Fraud

You can break the fraud chain.

Without you we can't do it.

FRAUD TRANSACTION PROTECTION

- **Fraud transaction protection specially for Accounts/Finance Team**

Implement the best practice of multifactor authentication by **confirming in person or over the phone before proceed the transaction for:**

1. Any email requests received from other employees to initiate Bank wire transactions.
2. All requests for Bank wire transfers or change in bank account details wiring instructions sent by email

- Review and reconcile all accounts/card statements: daily/weekly and monthly.
- Validate recipient account details and e-mail address before processing the transactions and be aware of phishing mails.

Secure your computer to prevent Internet Fraud

- Keep operating system software up to date.
- Keep Anti-virus software up to date and scan for issues regularly.
- Uninstall programs that are not used or unnecessary.
- NEVER give your password to anyone, even the help desk.
- Never leave your computer unattended.
- Do not install software from unknown sources.
- Do not connect with any free public WiFi anywhere.

Best Practice points for Information security

Reduce The Risk Of Human Error With Cyber Security Training Done Right

Even with a robust email security perimeter in place, attackers can try to bypass it and operate inside your email network. When you analyze the anatomy of most successful cyberattacks, nearly all of them have one thing in common. Some user, somewhere, did something that could have been avoided. In fact, research shows that human error is involved in 90%+ of all security breaches. If your employees aren’t ready for a cyberattack, the unfortunate truth is that your organization isn’t either

Best Practice points for Information security

- Be proactive and aware of phishing and internet fraud.
- Do not open attachments on e-mails that you did not expect. Be suspicious of emails purporting to be from a financial institution. Opening file attachments or clicking on web links could expose your system to malicious code that could hijack your computer.
- **Follow every instruction received from IT Team.**

Where to report Fraud /Phishing emails ?

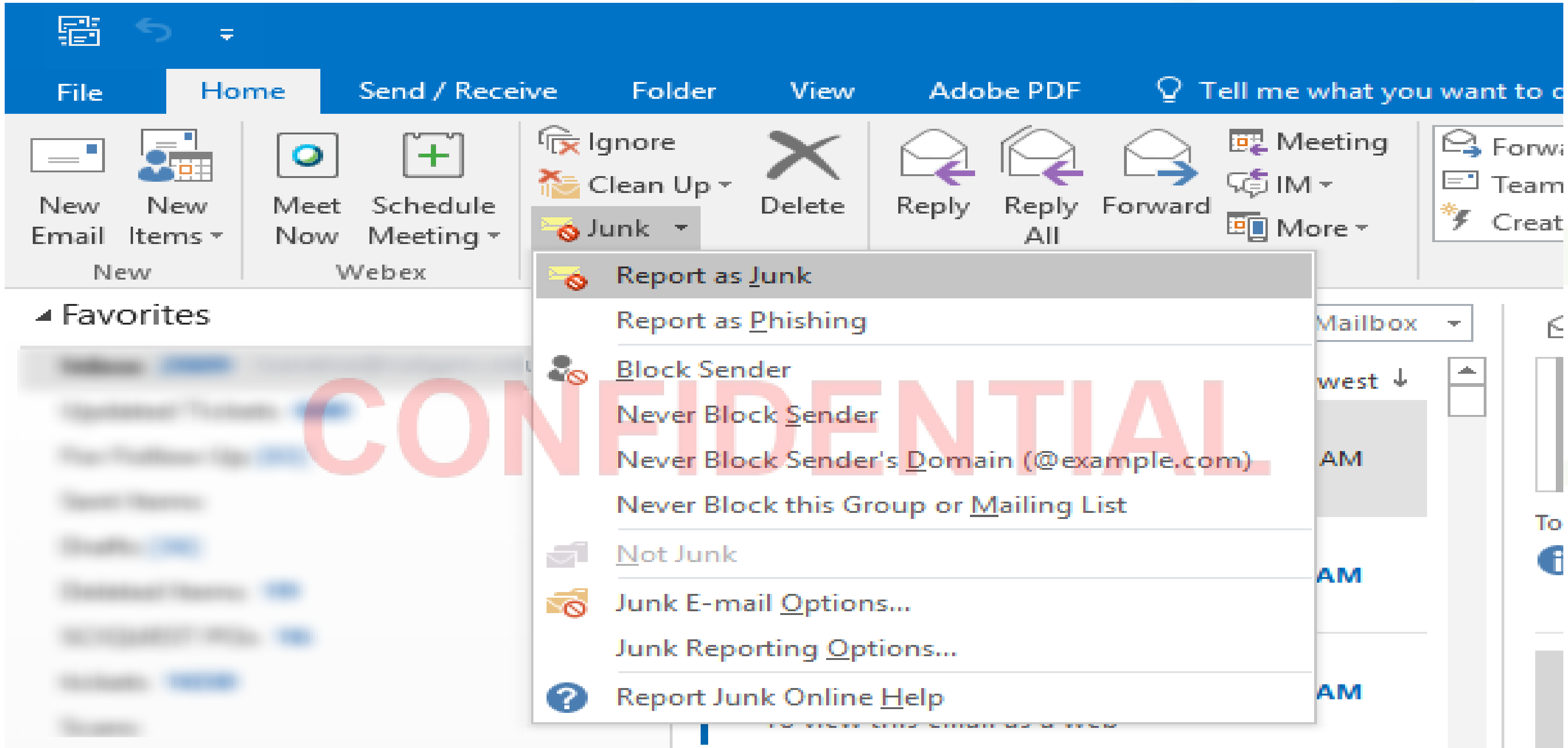
- Please report the phishing e-mails or suspicious activity to your immediate supervisor and IT Team.

- To report any phishing/internet fraud, you can also e-mail to :

devops@rxlogix.com

How to report phishing email on Outlook

1. In the message list, select the message or messages you want to report.
2. Above the reading pane, select **Junk** > **Phishing** > **Report** to report the message sender.



Any Questions ?

THANK YOU..!!

REVISION HISTORY

Version 01 Effective on 28-Aug-2020

1.0

DOCUMENT ELECTRONIC SIGNATURES

DOCUMENT APPROVAL WORKFLOW

Author Approval

Sanjeeb Kumar Chowdhury
Senior Manager - Support & Managed Services
Sanjeeb.Chowdhury@rxlogix.com

I am the author of this document.
Signed 7:08:49 AM UTC 14-Aug-2020

Required Workflow Steps for this Category

Sanjeeb Kumar Chowdhury
Senior Manager - Support & Managed Services
Sanjeeb.Chowdhury@rxlogix.com

RxLOGIX / Author
I am the author of this document.
Signed 7:09:22 AM UTC 14-Aug-2020

Jitender Sharma
Director of Engineering
Jitender.Sharma@rxlogix.com

RxLOGIX / Approver
I have reviewed and approve this document.
Signed 1:13:20 PM UTC 14-Aug-2020

Jayashree Acharya
Director
Jayashree.Acharya@rxlogix.com

RxLOGIX / Approver
I have reviewed and approve this document.
Signed 1:55:33 PM UTC 14-Aug-2020