To All Implementing Partners (IPs)

Ransomware is a type of malware that encrypts or blocks access to a victim’s data unless a ransom fee is paid. Cybercriminals gain access to a victim’s data by sending malicious emails, manipulating victims into revealing sensitive information, and injecting malware files into their devices. These attacks sometimes impersonate corporate or technical support and come via various channels, including SMS, voice calls, and WhatsApp messages.

Follow the steps below to protect yourself from ransomware attacks:

Keep your software up to date with the latest security patches.

Be cautious of email attachments and links from unknown sources.

Use strong, unique passwords and enable two-factor authentication.

Regularly back up your important data and store it securely.

Use reputable antivirus software and consider employing a firewall.

Do not reveal personal or financial information in unsolicited communications, including text messages or over the phone.

Be aware of any communications that try to make you act on impulse, such as by arousing strong emotions of alertness or fear of missing out.

If you experience any illicit or suspicious activity, please report it immediately by calling your company IT security provider or security contact person.