THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA
(Set up by an Act of Parliament)
VIJAYAWADA BRANCH OF SIRC OF ICAI

NEWSLETTER

For Private Circulation Only

January 2023

Managing Committee For the Year 2022-2023

CA. SRITHA SHIREEN GADDAM
CHAIRPERSON

CA. NARENDRA BABU VEERLA
VICE CHAIRMAN

CA. NITTA RAVI KISHORE
SECRETARY

CA. NARAYANA KANCHAMA REDDY
TREASURER

CA. U. LAKSHMI KRISHNA JAYANTH
SICASA CHAIRMAN

CA. VEMURU VEERA PAVAN KUMAR
MC MEMBER

CA. VENKATASUBBA RAO KOWTHA
MC MEMBER

• H A P P Y • N E W • Y E A R •

Happy
Pongal

May the almighty bless you all
with the best of health, wealth and prosperity.

vijayawada@icai.org, vjabranchofsircoficai@gmail.com
Contact : 9143224499
Phone : 0866 - 2576666

Safeguarding Digital Data

CA Narasimhan Elangovan, Partner, KEN & Co.

B.COM, FCA, CS, DISA, DIPIFR(UK), CISA(USA), LLB, CDPSE (USA), ISO 27001 Lead Auditor

Email: narasimhan@ken-co.in

The digital data has ingrained itself as an integral part of modern business.It has transformed the way business is conducted and opened grand vistas. With opportunity however, comes responsibility. The cyber world has unfortunately plenty of potential for someone with malicious intent. With remote working and increasing cyber attacks it is critical that we have measures to safeguard digital data.

Give below are a few regular and simple practices that can be followed to safeguard from Cyber Attacks and Risks.

Best Practices for Cyber Security

1. **Password Management:**
   Passwords are the first line of defence for any program. Having good passwords greatly enhances security whereas bad passwords may even negate the effects of other controls measures that are implemented.

   Best practices:
   - Ensure your passwords are strong and secure and use multi factor authentication where possible.
   - Regularly change passwords, and do not share them.
   - Consider using password Vaults for remembering multiple passwords for clients or self.
   - This can be also used for sharing the passwords with a designated set of individual, say the employees or teams who are working with Income tax, GST credentials.
   - Tools such as Zoho Vault, LastPass are quite useful

2. **System Access:**
   Controlling who has access to the system is perhaps the most obvious way to ensure security. Every person who has access to the system must.be a legitimate user. A legitimate user is one who has a valid reason for requiring access, whose identity can be verified and does not have malicious intent.

   Best Practices:
   - Remove system access from people who no longer need it, and limit access to only those needed to do their role.
   - Administrator privileges are provided on an “need to have” basis.
   - Regularly review the access privileges granted
   - Tools such as Manage Engine help in monitoring end point access

3. **Secure Wi-Fi & Devices**
   Wi-Fi, though greatly convenient, can pose a security threat for that very same reason. Extra care must be taken while using Wifi to ensure security.

   Best Practices
   - Secure your wireless network and be careful when using public wireless networks with mobile devices.
   - Avoid transacting online where you are using public or complimentary Wi-Fi.
   - Never leave your information physically unattended – secure your electronic devices.
   - Ensure employees have secured their home Wi-Fi devices. This includes changing default security credentials
   - Restrict guest access to only internet and not to the entire IT infrastructure of your office. A separate Wi-Fi profile may be created for the same.

4. **Legitimate Software:**
   Developing software is a complex process. Good software can have great functionality and ensure protection but faulty software could make an otherwise secure system vulnerable.

   Best Practices:
   - Only download/install programs from a trusted source.
   - Consider using application whitelisting so only authorised software applications run on your computer.
   - Disable untrusted Microsoft Office macros and block or uninstall Flash and Java.
   - Use only licensed software, as free software may open pandora's box.

5. **Patches and Anti-Virus:**
   Patches are updates to software. Patches are deployed by the software manufactures to not only enhance the software but to also increase security. Software patches must be updated at the earliest but care must also be taken that the patch does not lead to a disruption is business.

   Anti-Viruses are designed to prevent malicious software from entering the system and causing harm. An up to date Anti-Virus ensures the safety of the entire system.

   Best Practices:
   - Ensure all mobile devices/operating systems/software have the latest software updated.
   - Only legitimate and genuine licenses should be in place, and auto update features must be enabled.
   - Certain Anti-virus software or End point management software have facilities to track application updates and inform the administrator.

6. **Clean devices:**

Though great for carrying legitimate information, USBs could also be a carrier of viruses or other forms of malware. Care must be taken to ensure that the system is not compromised by unfamiliar information portability devices.

Best Practices:

- Do not use USB or external hard drives from an unfamiliar source.
- Preferably block USB usage and use only in restricted machines for the purposes of digital signature and encrypted USBs.
- Prefer sharing data over encrypted channels such as Secured file transfer protocols, or secure Cloud applications.

7. **Social Media:**

Social media is one of the most literal manifestations of the saying "the world at our fingertips". Sensitive content once released onto social media is almost impossible to erase.

Best Practices:

- Be vigilant about what you share on social media – try to keep personal information private and know with whom you interact online.
- Disable locations sharing, third party access to your profile and regularly verify your Privacy controls.

8. **Email:**

Emails has allowed communication to occur at the speed of thought. But it has also created the information explosion.

Best Practices:

- Use a spam filter for your email and use email carefully - be wary of downloading attachments or opening links in emails you have received in case it is a 'phishing' attempt.
- Using paid and encrypted email accounts can be more beneficial.

9. **Regular Backups:**

Data can be volatile. It's easier than you would expect to lose data. Maintainingat least one detailed copy of all important data is maintained at a secure location ensures robustness.

Best Practices

- Use off-line, incorruptible, and disconnected backups.
- Prefer the usage of automated back-up in addition to external hard disks backing up the data.

10. **Bring Your Own Devices:**

The use of personal devices for work has been a trend that has picked up greater momentum is recent years with the advent of smartphones, tablets and other such devices with high

computational capabilities. It has also brought about an increase in the number of devices that must be taken into consideration for the purpose of security.

Best Practices:

- In case of employees bringing their own device, it is highly recommended that a thorough checks are performed on those systems prior to giving access. Such checks include checking if the laptop is genuine, the operating system, anti-virus software is in place and unsolicited software are not downloaded.
- Declaration may be taken from employees regarding the careful usage of the data and adherence to office policies.
- Separate user account may also be used, and data loss prevention tools may be deployed.

Conclusion

The above mentioned practices are just the beginning. Due to the inherent complexity of the cyber environment, new threats are created just as fast as security measures can be developed. The perpetual race between threats and security controls is bound to continue. It is ever important that we maintain vigilance and keep ourselves updated of the new possibilities and dangers.

CA Srinivasa Rao Eluri
M.Com., FCA
Partner
Eluri & Associates | Chartered Accountants
reached at: info@sreluri.in | 9440325485

Updates are collected from various online sources

Dear Members, wishing u all a very Happy New Year 2023

The Institute of Chartered Accountants of India	
ICAI Members' Journal	http://anax8a.pressmart.com/TheCharteredAccountant
Leaders in the Profession	ICAI and CNBC TV18 have come together to celebrate the spirit of excellence of 40 dynamic Chartered Accountants under the age of 40 who have emerged as leaders in the profession and are setting an example for others to follow.
Peer ReviewBoard	is organising a One day Training Programme for Peer Reviewers on 21st December 2022 being hosted by Gautam Budh Nagar branch of CIRC of ICAI at Gautam Budh Nagar branch
ICAI members are known to you to comply with the mandatory CPE hours' requirements for the Calendar Year 2022 and block period (2020-2022) till 31st December 2022	https://icai.org/post/continuing-professional-education-committee.
MEF	Draft Bank Branch Auditors' Panel (MEF) of Chartered Accountants/firms for the year 2022-23 has been hosted at

Ministry of Corporate Affairs	
MCA Notification	MCA is launching the Second set of Company Forms covering 56 forms in two different lots on MCA21 V3 portal. 10 out of 56 forms will be launched on 09th January 2023 at 12:00 AM and the remaining 46 forms on 23rd January 2023. Following forms will be rolled-out on 09th January 2023, SPICe+ PART A, SPICe+ PART B, RUN, AGILE PRO-S, INC-33, INC-34, INC-13, INC-31, INC-9 and URC-1. To facilitate implementation of these forms in V3 MCA21 portal, stakeholders are advised to note the following points: 1. Company e-Filings on V2 portal will be disabled from 07th January 2023 12:00 AM to 08th January 2023 11:59 pm for 10 forms which are planned for roll-out on 09th January 2023. 2. Company e-Filings on V2 portal will be disabled from 07th January 2023 12:00 AM to 22nd January 2023 11:59 pm for 46 forms which are planned for roll-out on 23rd January 2023. 3. All stakeholders are advised to ensure that there are no SRNs in pending payment and Resubmission status.

Scan QR Code for Monthly Updates

Click Here to Read

COMPLIANCE UPDATES FOR JANUARY 2023

CA K Ramgopal
ramgopalk@hotmail.com

S.No	Particulars of Compliance	Act	Forms/ Returns	Due Date
1	Due date for deposit of tax deducted/collected for the month of December, 2022. (TDS & TCS). However, all sum deducted/collected by an office of the government shall be paid to the credit of the Central Government on the same day where tax is paid without production of an Income-tax Challan.	Income Tax		07-Jan-23
2	Form GSTR-7 for the month of December 2022	GST	GSTR-7	10-Jan-23
3	The due date for furnishing statement by e-commerce companies for the month of December 2022	GST	GSTR-8	10-Jan-23
4	Return of outward supplies of taxable goods and/or services for the Month of December 2022 (for Assesses having turnover exceeding 1.5 Cr.) Monthly Return.	GST	GSTR -1	11-Jan-23
5	Return of outward supplies of taxable goods and/or services for the Quarter Oct - Dec 2022 (for Assesses under QRMP)	GST	GSTR 1 IFF	13-Jan-23
6	GST Return for input service distributor for the month of December 2022	GST	GSTR 6	13-Jan-23
7	ESIC Payment for December 2022	ESIC	ESI Challan	15-Jan-23
8	Due date for issue of TDS Certificate for tax deducted under Section 194-IA in the month of November, 2022	Income Tax		15-Jan-23
9	Due date for issue of TDS Certificate for tax deducted under Section 194-IB in the month of November, 2022	Income Tax		15-Jan-23
10	Due date for furnishing of Form 24G by an office of the Government where TDS/TCS for the month of December, 2022 has been paid without the production of a challan	Income Tax	Form 24G	15-Jan-23
11	Quarterly statement of TCS deposited for the quarter ending September 30, 20122	Income Tax		15-Jan-23
12	Due date for uploading declarations received from recipients in Form No. 15G/15H during the quarter ending September, 2022	Income Tax		15-Jan-23
13	PF Payment for December 2022	PF	ECR	15-Jan-23
14	Simple GSTR return for Composition Dealers for Quarter ended December 2022	GST	CMP-08	18-Jan-23
15	Simple GSTR return for the month of December 2022	GST	GSTR 3B	20-Jan-23
16	Summary of outward taxable supplies and tax payable by Non-Resident taxable person & OIDAR.	GST	GSTR-5 & 5A	20-Jan-23
17	PF Return filling for December 22 (including pension & Insurance scheme forms.	PF		25-Jan-23
18	Due date for furnishing of challan-cum-statement in respect of tax deducted under Section 194-IA in the month of December, 2022	Income Tax		30-Jan-23
19	Due date for furnishing of challan-cum-statement in respect of tax deducted under Section 194-IB in the month of December, 2022	Income Tax		30-Jan-23
20	Quarterly statement of TDS deposited for the quarter ending September 30, 2022	Income Tax		31-Jan-23

PHOTOS IN EVENTS

Career Counselling

DHMC School 27-12-2022



DR.J.D.M.MC.High School 28-12-2022



Gandhihi Mahila Kalasala


Lakireddy Hanimireddy degree college 03-12-2022





Nalanda Degree College



Netaji High School 28-12-2022




SDMYRR School


STR School 27-12-2022


Triveni Degree College 26-12-2022





Triveni Jr.College 26-12-2022



Industrial Tour@ VM Bakery- 21-12-2022





Industrial Tour @ Vijaya Milk Project 02-12-2022



One day CPE Seminar

Three day Workshops 15,16,17 Dec

VCM on Walkthrough on Networking guidelines of ICAI @ 22-12-2022

VCM on Multi DisiplinaryPartenership firms - A way forward@ 23-12-2022

VCM on Awareness Program on Audit Quality Maturity Model @ 26-12-2022

VCM on Code of ethics & disciplinary mechanism with practical case laws @ 27-12-2022

SICASA Day Celebrations 1-12-2022

Youth Fest