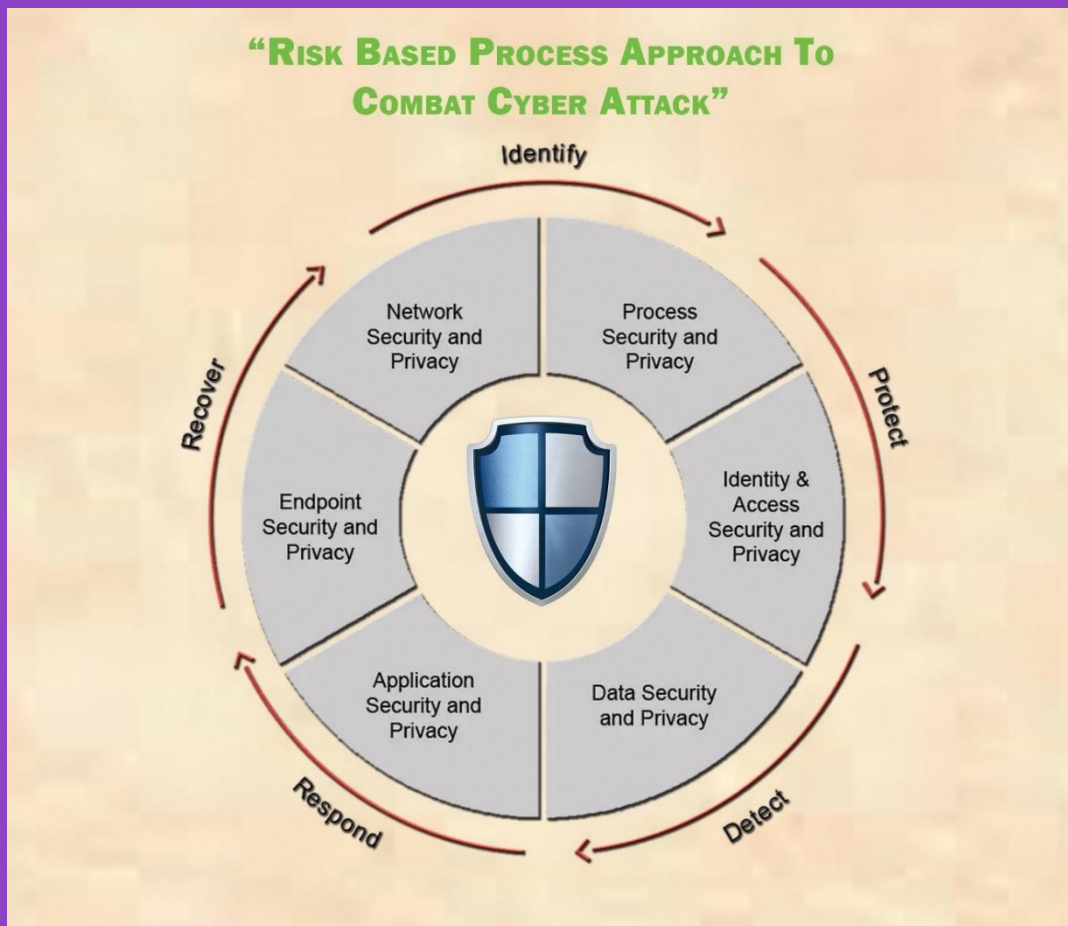




Cyber Safe Bengal – Cyber Safe India

Cyber Security Centre of Excellence (CS-CoE)

Department of Information Technology & Electronics
Government of West Bengal





Cyber Security – Centre of Excellence

Helping to make West Bengal the safest place to live and work online

Cyberspace has become a dynamic and integral part of our society, propelling economic growth and enriching our lives in countless ways. The internet has connected us to people across the globe without physical boundaries. With the ease of technology, Cyberspace provides an opportunity for criminals to interfere with individuals and businesses. In this era of internet, prevention of cyber-attacks and protection of our systems, networks and data is one of the biggest challenges which every nation is facing.

To cater to the aforementioned challenges, the state of West Bengal in India established the West Bengal Cyber Security Center of Excellence (WB-CSCoE) to prepare the state for effectively dealing with cyber offences/incidents". The Cyber Security Centre of Excellence (CS-CoE) runs its operations under the guidance of the Department of Information Technology and Electronics, Government of West Bengal. The main purpose of CS-CoE is to create awareness on Cyber Security amongst Govt. officials as well as citizens of the state.

The 5 fundamental blocks of CSCoE activities are:

- Awareness Generation & Capacity Building
- Cyber Security Assurance
- Security Operation Center (SOC)
- Cyber Forensic & Investigation
- Research & Development , Advisory

Cyber Security Centre of Excellence
Webel Bhavan, Ground Floor, Block – EP & GP, Sector – V, Bidhannagar, Salt Lake, Kolkata – 700 091
Phone No.: 033 2357-5218, email: cscoe@wb.gov.in, Web: cscoe.itewb.gov.in

CYBER SAFE BENGAL – CYBER SAFE INDIA



Password length should be minimum 10 characters using a combination of letters, numbers and special characters

1

2

3

Don't use the common passwords such as Name of family, pets, friends, birthdays etc.

4

5

6

Enable password protection for sensitive documents.

7

8

9

Don't use old passwords. Re-used passwords are easier to crack through observing key-log patterns or through social engineering

10

11

12

Be careful when entering passwords in front of others. Don't let others watch while log in or doing online transaction

13

14

15

January Planner

16

17

18

Change your password immediately you suspect it has been compromised. Report suspicious activity to the IT team

19

20

21

Don't store passwords in readable form in computers, notebook, notice board etc.

22

23

24

Don't keep open files containing personal or confidential information on your desks

25

26

27

Always log-off your computer when leaving it unattended with "windows + L" or "Ctrl+Alt+Del"

28

29

30

31

Avoid disclosing any information on untrusted phone calls, meetings or emails. Attackers often pose as genuine people to gain confidential official information to cause a data breach

Use of Anti-virus is mandatory

1

2

3

Anti-virus should only be licensed software application

4

5

6

Anti-virus software available for free download should not be installed

7

8

9

Screensaver with timeout period of maximum 2 minutes should be enabled

10

11

12

Do not use using public computers/ cyber cafes' for office work

13

14

15

February Planner

16

17

18

Do not download unnecessary programs from anywhere, even from legitimate trusted sources

19

20

21

Do not click on untrusted links even if they appear to be from a legitimate source

22

23

24

When on tour, don't use the services that require location information

25

26

27

Always scan all removable media with antivirus

28

29

Avoid phone calls/ emails/ SMS regarding unknown inheritance, foreign lottery, fund transfer from foreign country, etc. These are example of scam to get information or money from you



CYBER SAFE BENGAL

Don't conduct any financial transactions by using public computers or public Wi-Fi connections

1

2

3

In public Wi-Fi there is a risk that your information can be read by unauthorized people

4

5

6

Try to encrypt the data before copying into removable storage media

7

8

9

Always use WPA2 or higher encryption in wireless

10

11

12

Don't disclose your identity, change the default network device name /SSID (service set identifier)

13

14

15

March Planner

16

17

18

Change the default password of network device

19

20

21

Activate MAC id filter to avoid unauthorized access

22

23

24

Sudden power cuts may result in loss of data or non-recovery of important systems due to corruption of operating systems files

25

26

27

Power supply should be controlled through UPS or Surge Protector

28

29

30

31

All employees, contractual staff, consultants, partners, third party staff etc. SHALL NOT Disclose official information on social media portals or applications



CYBER SAFE BENGAL

Do not open untrusted links & attachments

1

2

3

Avoid phishing attacks – do not open untrusted emails

4

5

6

Do not open email attachments which do not seem relevant to any ongoing official communication

7

8

9

Avoid vishing attacks

10

11

12

Do not reveal any sensitive information over phone calls unless the source is completely verified and trusted

13

14

15

April Planner

16

17

18

If any message or email conveys a sense of urgency, seems to apply high pressure sales tactics, be careful of opening or clicking on any link / attachment

19

20

21

Avoid phone calls/ emails/ SMS regarding unknown inheritance, foreign lottery, fund transfer from foreign country, etc.

22

23

24

Anti-virus software available for free download should not be installed

25

26

27

Try to get a full assurance as to the identity of the caller prior to disclosing any vital information

28

29

30

Ask for some verifiable credential such as name of immediate senior (if the caller poses as an official of another Government Department)



CYBER SAFE BENGAL

Respect the privacy of others, just as you expect the same from them

1

2

3

Beware of external wires of devices connected to swiping machines

4

5

6

Use Internet Ethically. Avoid misusing the intended use of the internet

7

8

9

Ensure that you have policies to protect the confidentiality and integrity regarding the use of e-mail and internet

10

11

12

Do not log on to any e-mail account other than yours even if requested to do so

13

14

15

May Planner

16

17

18

Do not send e-mail messages from another user mail box

19

20

21

Do not use copyrighted software without the author's permission

22

23

24

It is illegal to duplicate / distribute software or its documentation without the permission of the copyright owner

25

26

27

Consult your authorities if you are unsure about the use of a particular software product

28

29

30

31

Stealing other's information by using computers / Mobiles is a crime. Stealing should not be considered different just because a computer is involved



CYBER SAFE BENGAL

Downloading copyrighted software, games / books etc without owner's permission is unethical and can have major legal implications

1

2

3

Keep an eye on children when they use the internet

4

5

6

Discourage children from online chat with strangers

7

8

9

Pay close attention to the strength of the password used for your bank account

10

11

12

Changing your password regularly adds strength and protection from frauds and hacking

13

14

15

June Planner

16

17

18

Never use other's computers to modify information such as password / documents etc.

19

20

21

Ensure that you are safe from internet attacks

22

23

24

Use updated anti-viruses, anti-spyware software

25

26

27

Secure your computer with latest operating system and updated patches

28

29

30

Use secured browsers for financial transactions



CYBER SAFE BENGAL

Intentionally or unintentionally, do not disclose sensitive information to others unless they have a business need to know

1

2

3

Never give system or network information to strangers

4

5

6

Report any suspected / unauthorised access of computer systems to your Technical Support Team

7

8

9

If you feel your system activity is abnormal, immediately inform your Systems support members to monitor the system

10

11

12

Encourage family members to follow the rules and guidelines for using internet safely

13

14

15

July Planner

16

17

18

Never give financial information to unknown websites on the internet

19

20

21

Never respond to messages that are threatening or make you feel uncomfortable

22

23

24

Never meet online friends in person without family authorisation

25

26

27

Online friends are strangers and there is no guarantee that the person on the other side is saying the truth

28

29

30

31

Make sure to set your profile to private on social networking sites so that strangers cannot view your personal information



CYBER SAFE BENGAL

Never download files through CHAT sessions from unknown persons

1

2

3

The files shared during chat session may contain harmful virus that may damage your system

4

5

6

Unless you know the sender and know the contents of the file, avoid downloading them

7

8

9

Always avoid chatting with unknown persons in internet and avoid getting carried away with unsolicited links during chatting

10

11

12

Always read carefully about "Terms & Conditions" before confirming anything over internet

13

14

15

August Planner

16

17

18

New viruses creep upon a daily basis. It is important that we do back-up our valuable data files regularly

19

20

21

Do install an anti-virus software program and update it often as there are new viruses discovered everyday

22

23

24

Scanning the attachments will prevent you from downloading virus affected contents

25

26

27

Configure your e-mail client to scan attachments automatically before any download

28

29

30

31

For secure browsing, follow the best practice of internet browsers. Delete cookies, block pop-ups, delete temporary files and history after completion of the session



CYBER SAFE BENGAL

Educate yourself on best practices, guidelines on internet usage

1

2

3

When you receive a warning from the antivirus, clean the virus immediately

4

5

6

Never trust the icons of attachment files. The virus file may be shown as PDF file

7

8

9

Never open web-links in your e-mail. Always type links in Web browser

10

11

12

Always use e-mail transaction through secured e-mail sites

13

14

15

September Planner

16

17

18

Always close all the applications while doing online transactions

19

20

21

The cyber world is open to all. Anyone can post data on internet. Beware of false information

22

23

24

Do not respond if you are prompted to save your login details

25

26

27

Never leave your computer unattended when you are connected to any internet banking site

28

29

30

Be suspicious of any unexpected demands on the net for your personal information. No bonafide companies ask for this information without reason



CYBER SAFE BENGAL

Always set the safe search filtering option to strict mode which helps you to stop or display any unwanted data

1

2

3

Always use spam filters in e-mail. By using the spam filter in e-mails, you can combat the flow of unwanted e-mails

4

5

6

Make sure that your online transactions are encrypted. Encryption prevents the attacker to view the information

7

8

9

Instead of directly clicking on the URL, it is always better to type the required URL in the browser

10

11

12

Update the web browser before browsing internet

13

14

15

October Planner

16

17

18

Block Popup of windows while browsing internet because viruses are embedded within the popup windows

19

20

21

Make sure you do not use remember password option in browser

22

23

24

Always clear the browser history and cache before you leave a system in internet centres

25

26

27

Always check the authenticity of the person before you accept a request in Social Networking

28

29

30

31

Do not pursue links that offer online scan of your PC and offer free download of those software. Ignore such links



CYBER SAFE BENGAL

Always set the options in antivirus to check for your online activities so that it detects unwanted downloads

1

2

3

Content filters are very useful for children, parents and teachers. They work as web boundaries

4

5

6

Use content filters to prevent access to websites that are considered unsuitable

7

8

9

Avoid subscription services on internet unless there is a good business reason for subscribing them

10

11

12

Ensure the card is swiped in your presence

13

14

15

November Planner

16

17

18

Please remember to take your Debit/Credit Card back after completing your ATM transaction

19

20

21

Never reply to lottery e-mails. If you get lottery e-mails without your intervention, ignore them

22

23

24

Don't write your passwords anywhere

25

26

27

Use different passwords for different services while browsing

28

29

30

Be cautious while downloading the applications through Bluetooth or as an MMS attachment. Mobile phone virus spreads through MMS attachment and Bluetooth transfer



CYBER SAFE BENGAL

Never use your name or nick name as your password because it becomes easy to crack it

1

2

3

Be careful when you are posting personal information in global address groups. Phishing attacks can be done by hacker using this information

4

5

6

Be careful with credit card transaction for online shopping. Check whether the site is secured

7

8

9

Before transaction, delete cookies and don't save credit card details in the website while you do online shopping

10

11

12

Verify the security of website for online payment system

13

14

15

December Planner

16

17

18

Never keep your credit card and PIN at one place. Keep them at safe places separate from each other

19

20

21

Always sign on the back of the credit card as soon as you receive it

22

23

24

Never leave your computer unattended when connected to your secure internet banking site

25

26

27

Make sure your logout of the site specifically when you finish your internet banking session

28

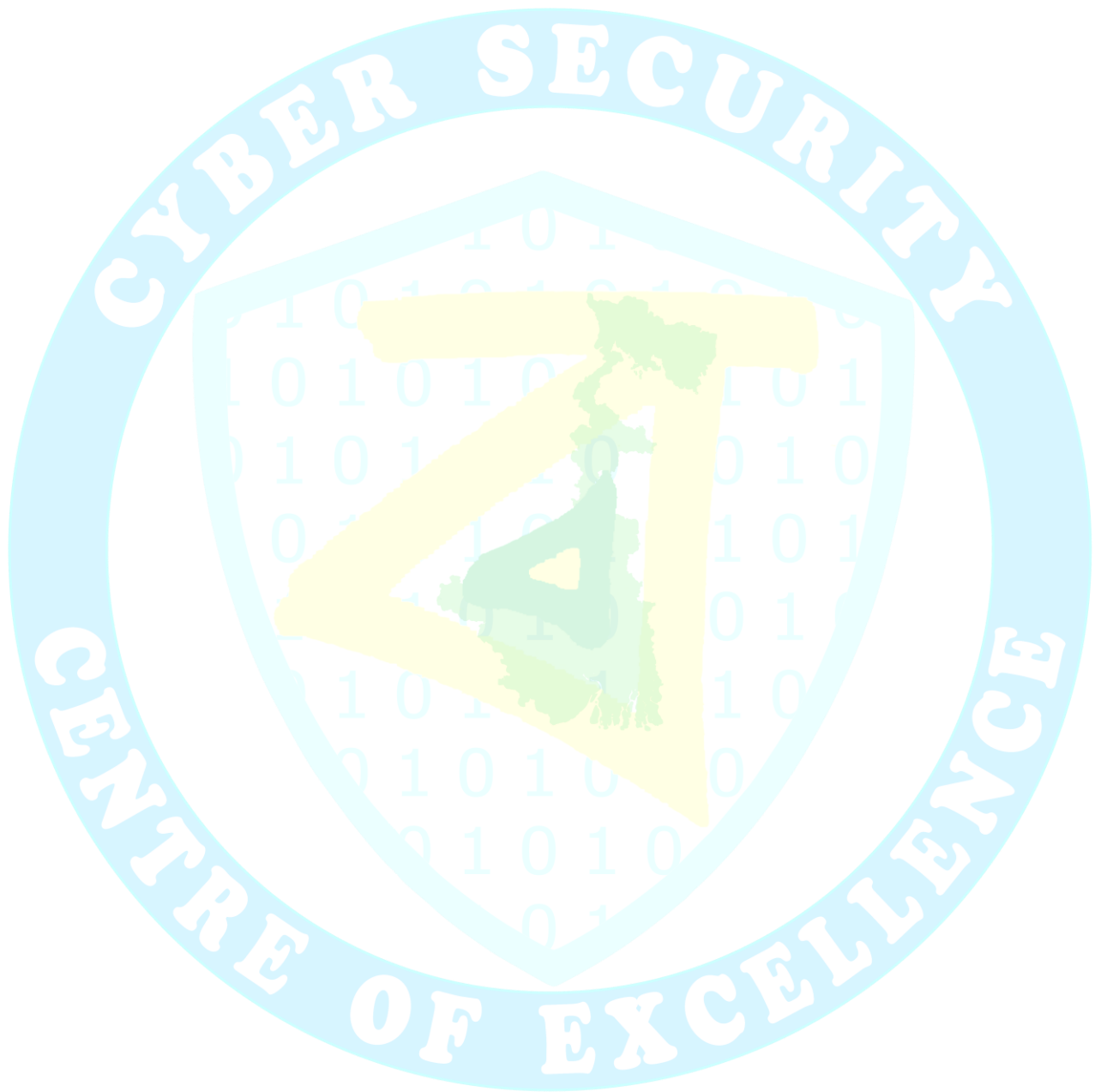
29

30

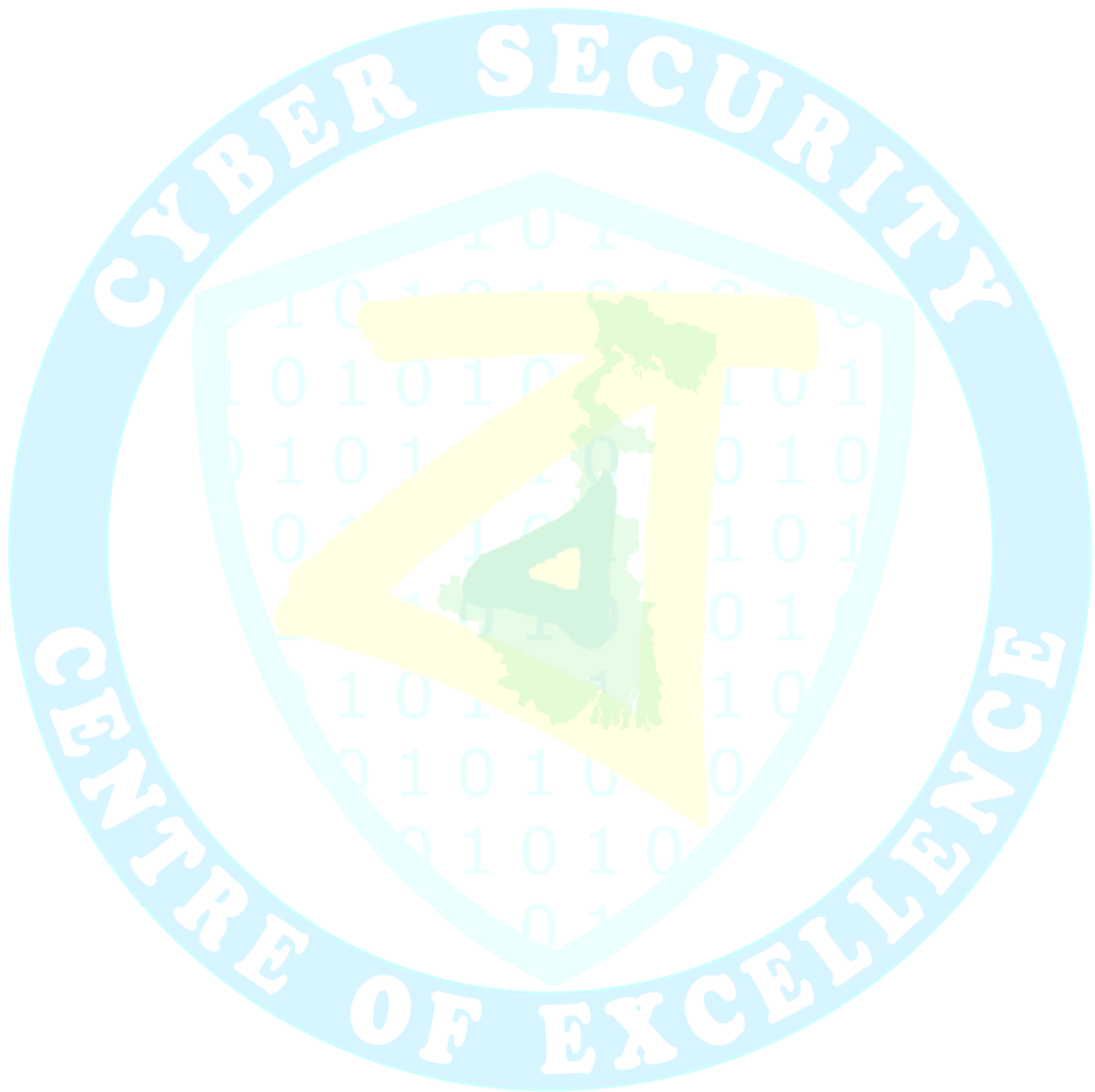
31

Always signup for SMS and e-mail alerts for every transaction to ensure that there are no transactions without your knowledge

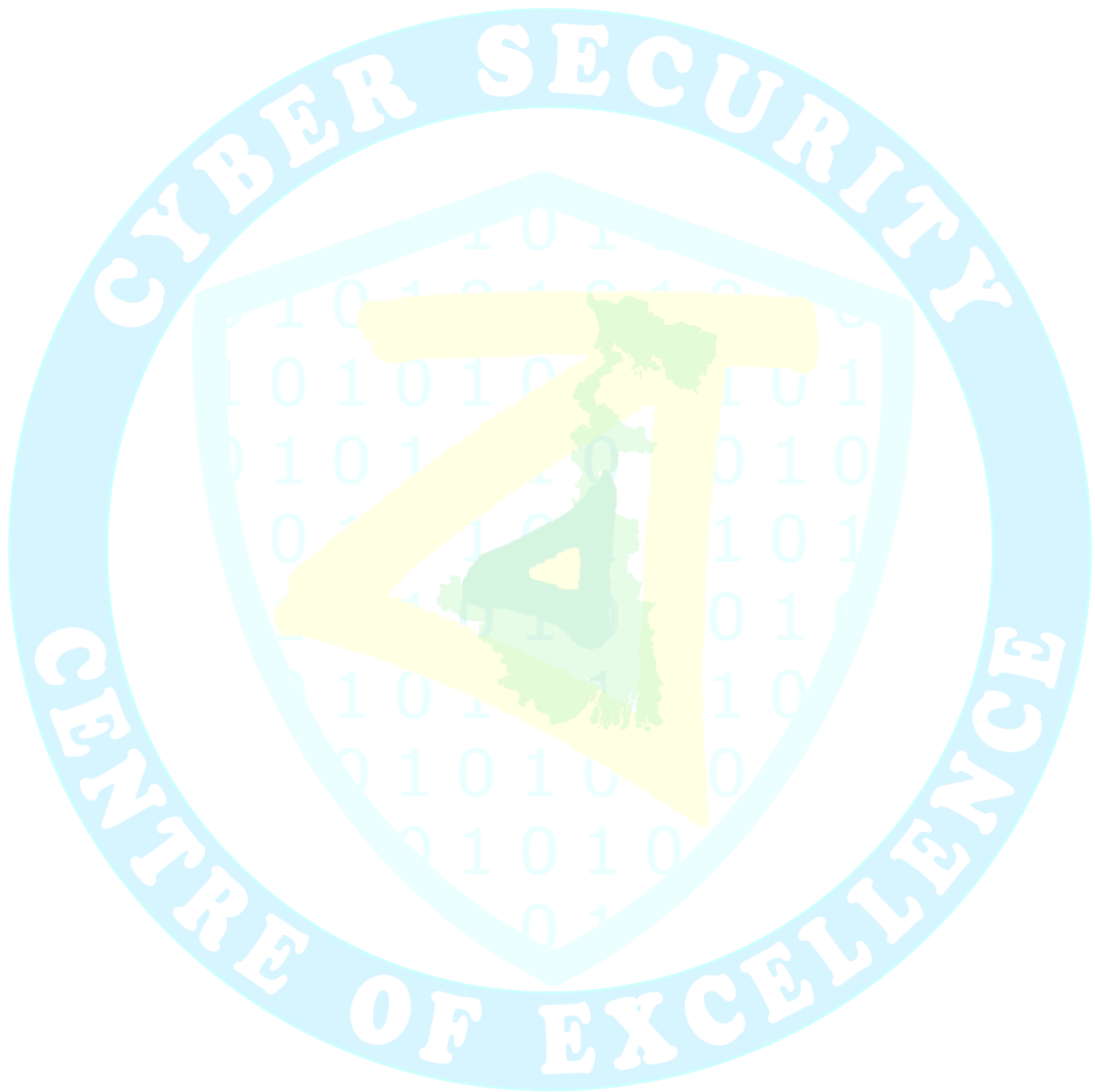
INTENTIONALLY LEFT BLANK



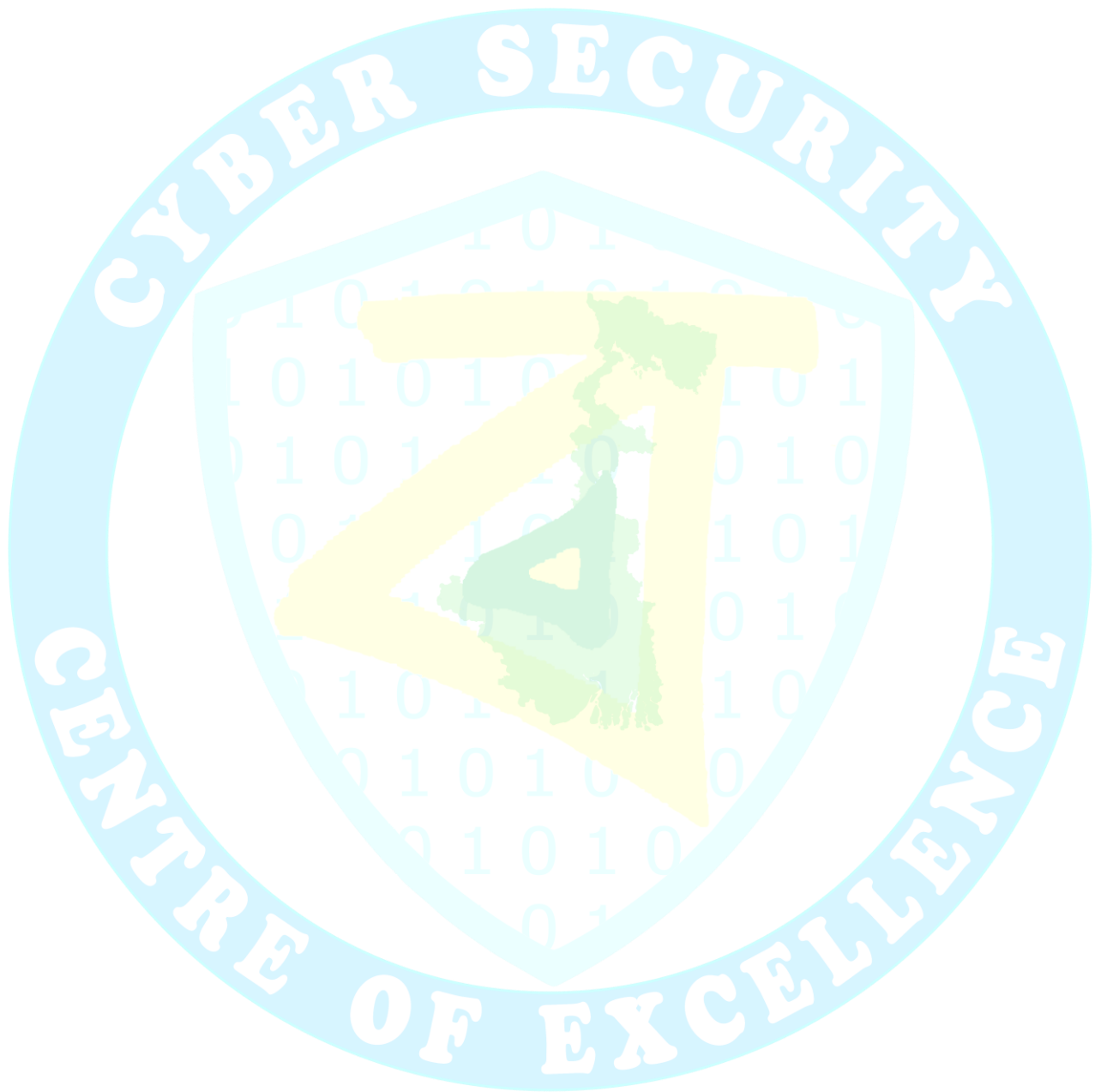
CYBER SAFE BENGAL



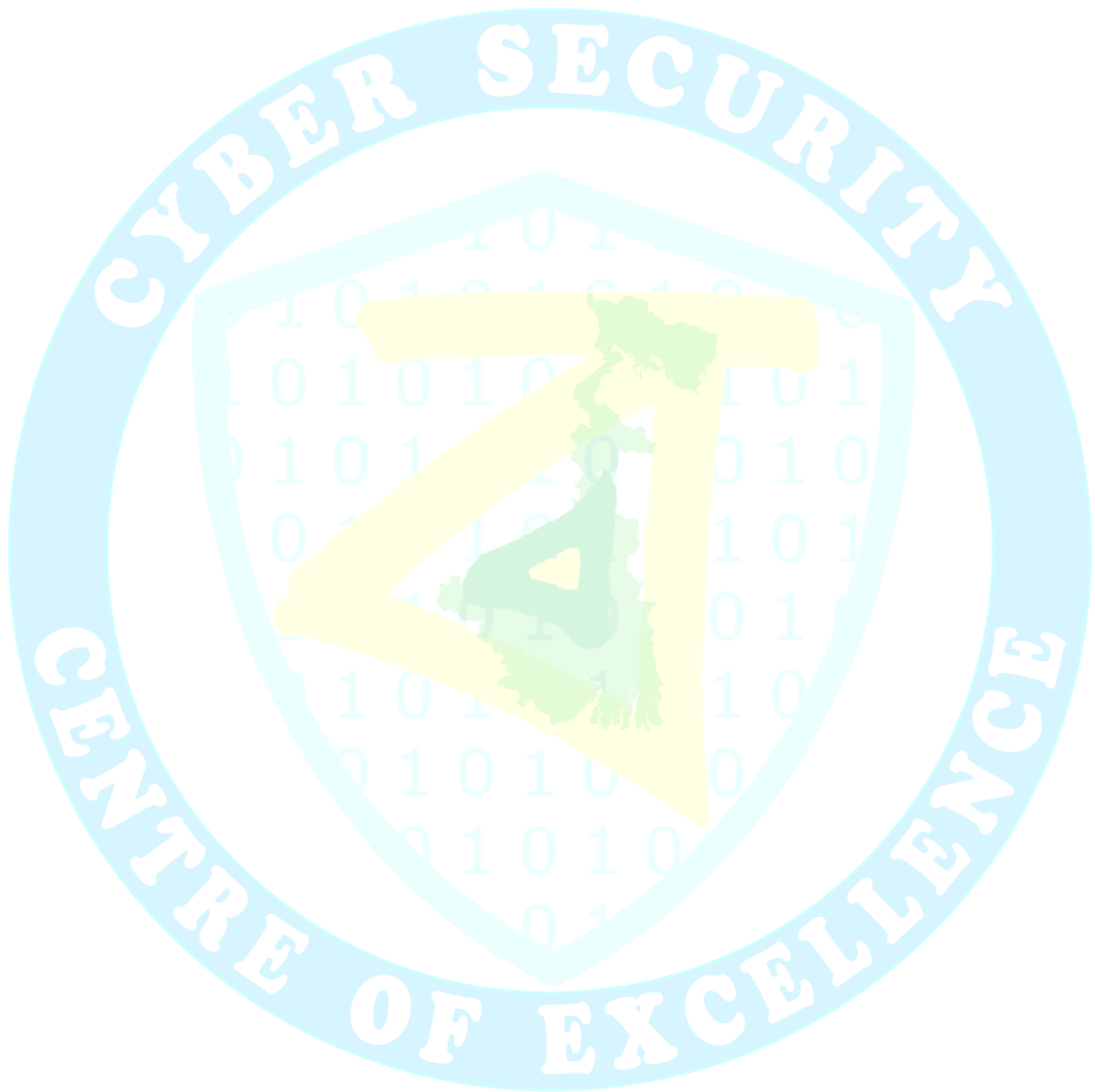
CYBER SAFE BENGAL



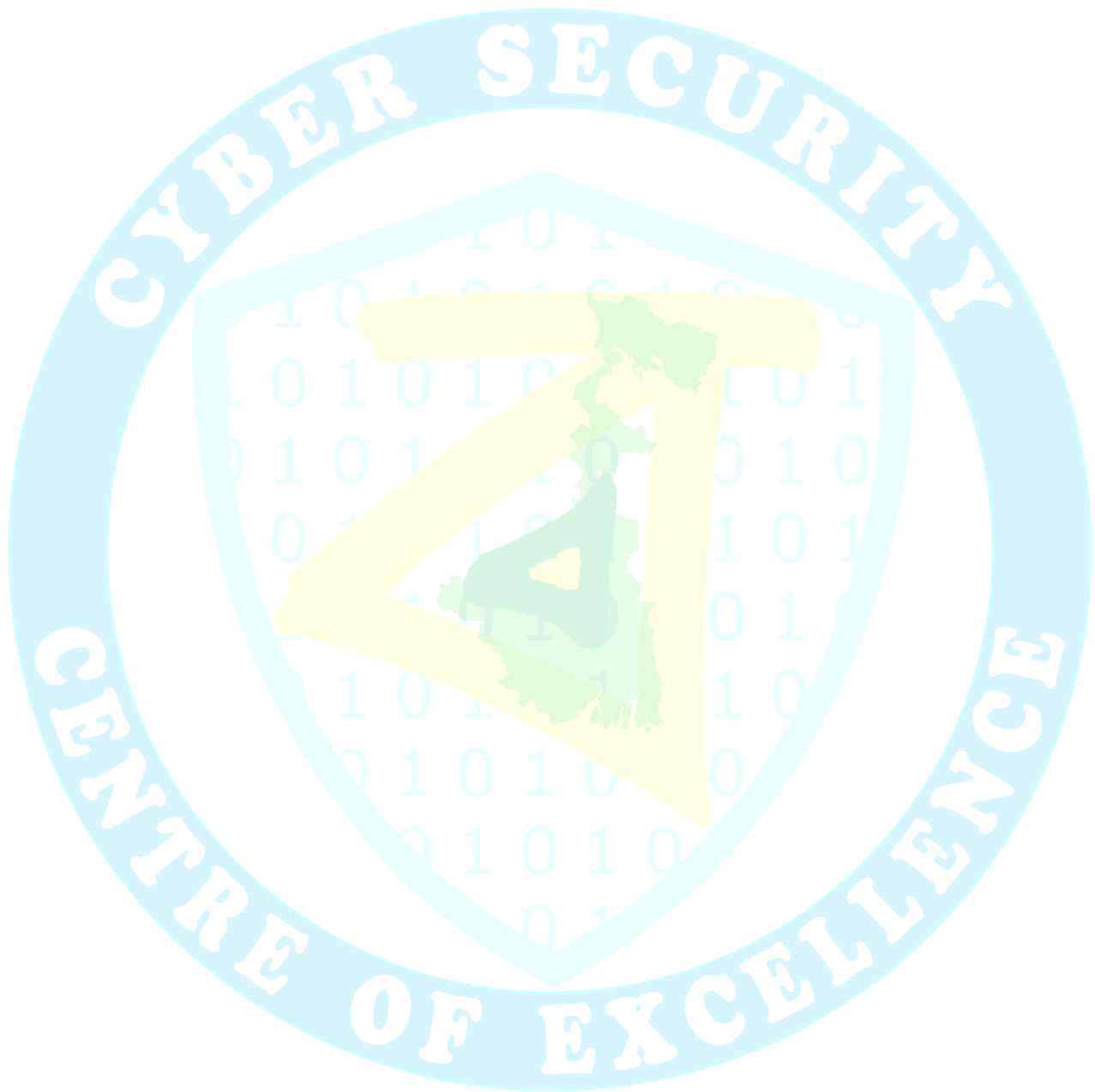
CYBER SAFE BENGAL



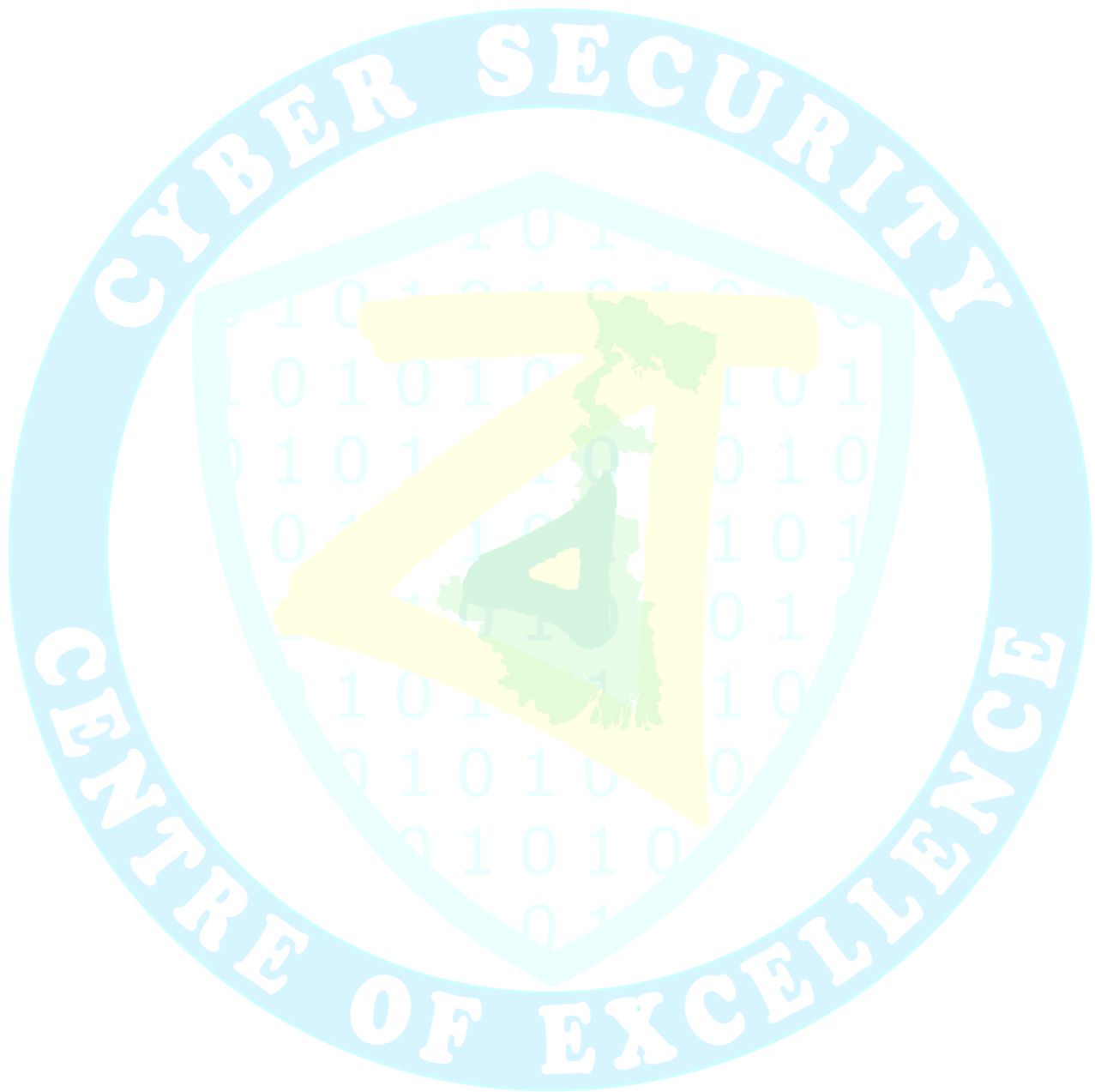
CYBER SAFE BENGAL



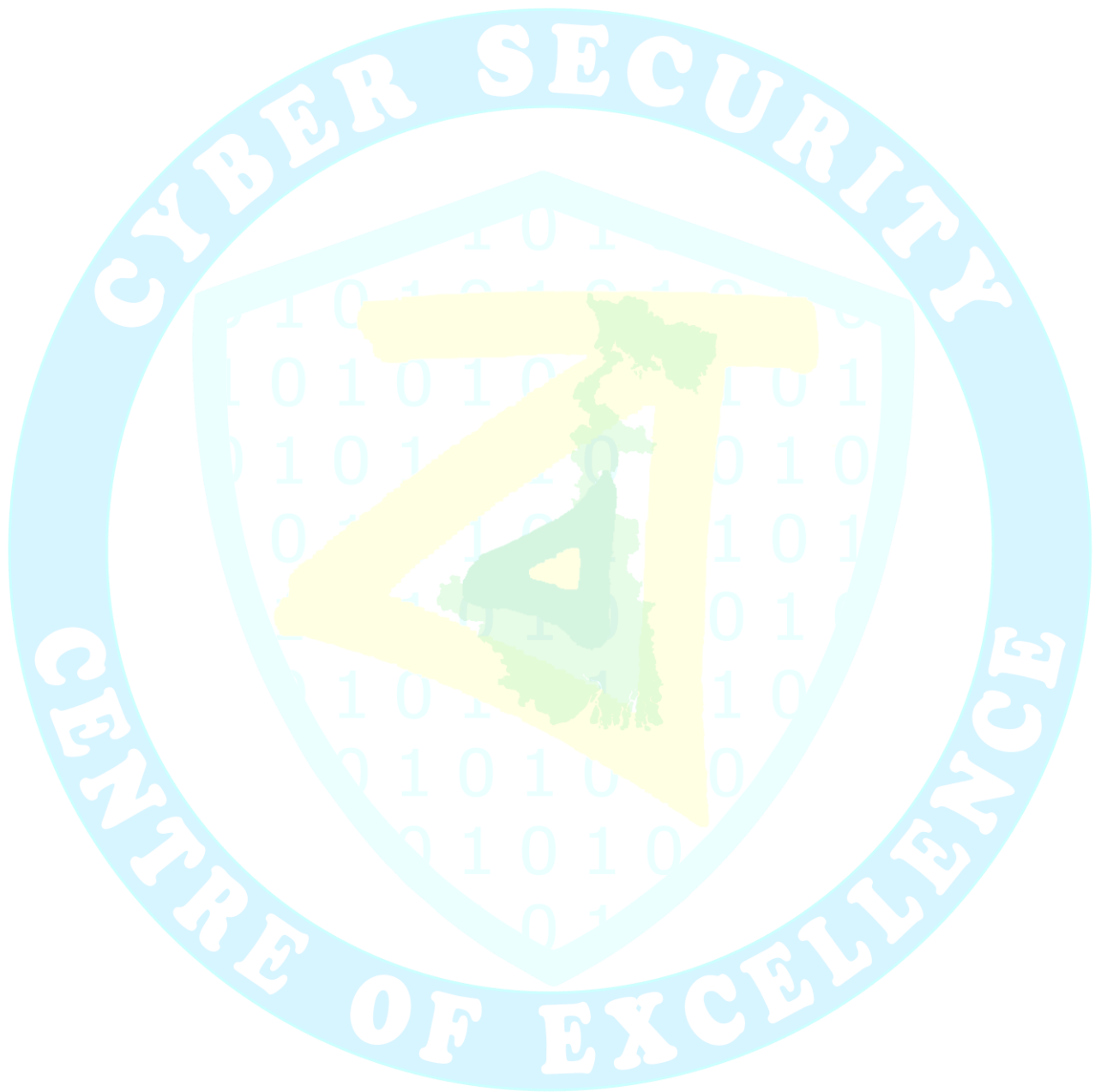
CYBER SAFE BENGAL



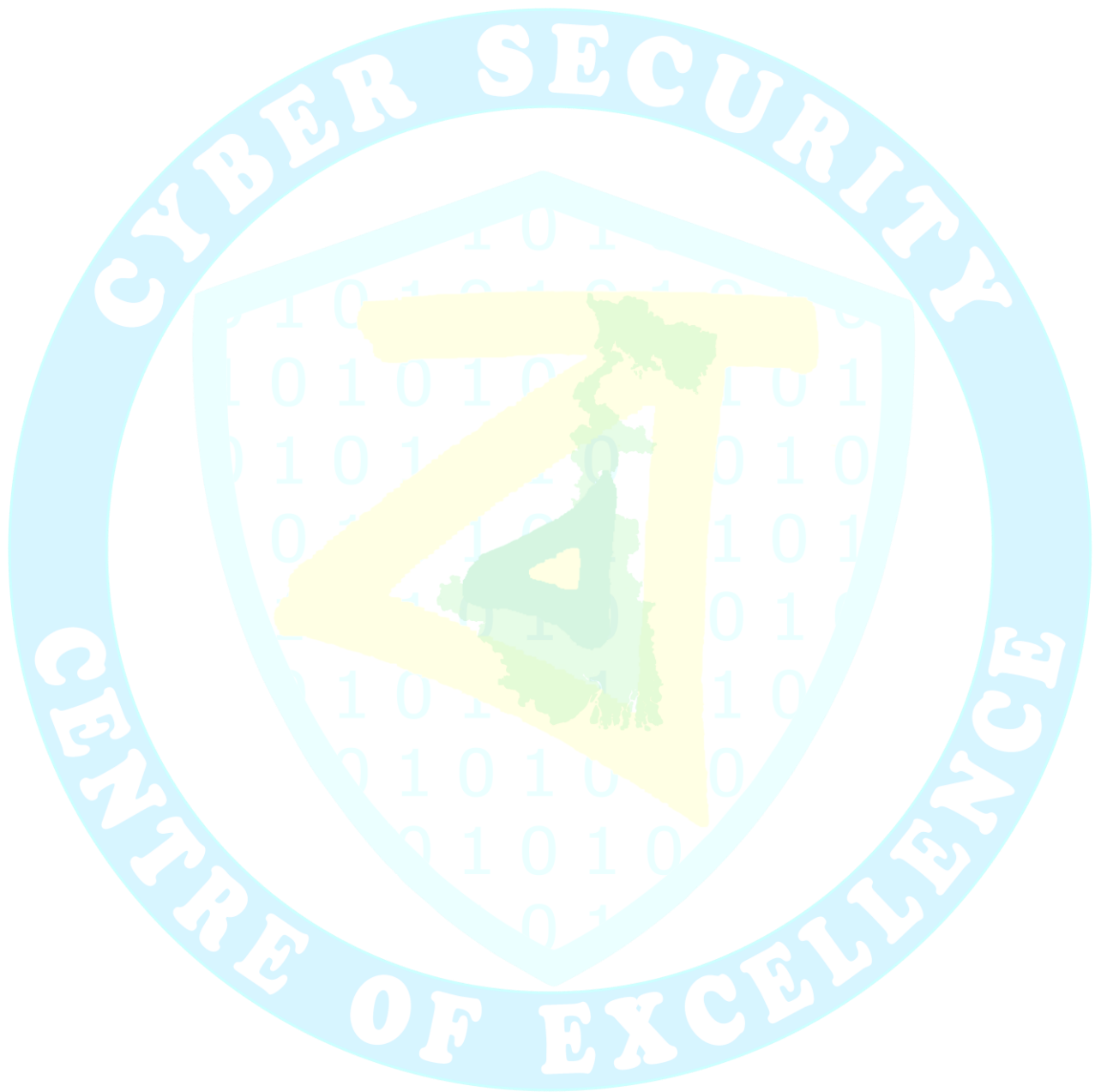
CYBER SAFE BENGAL



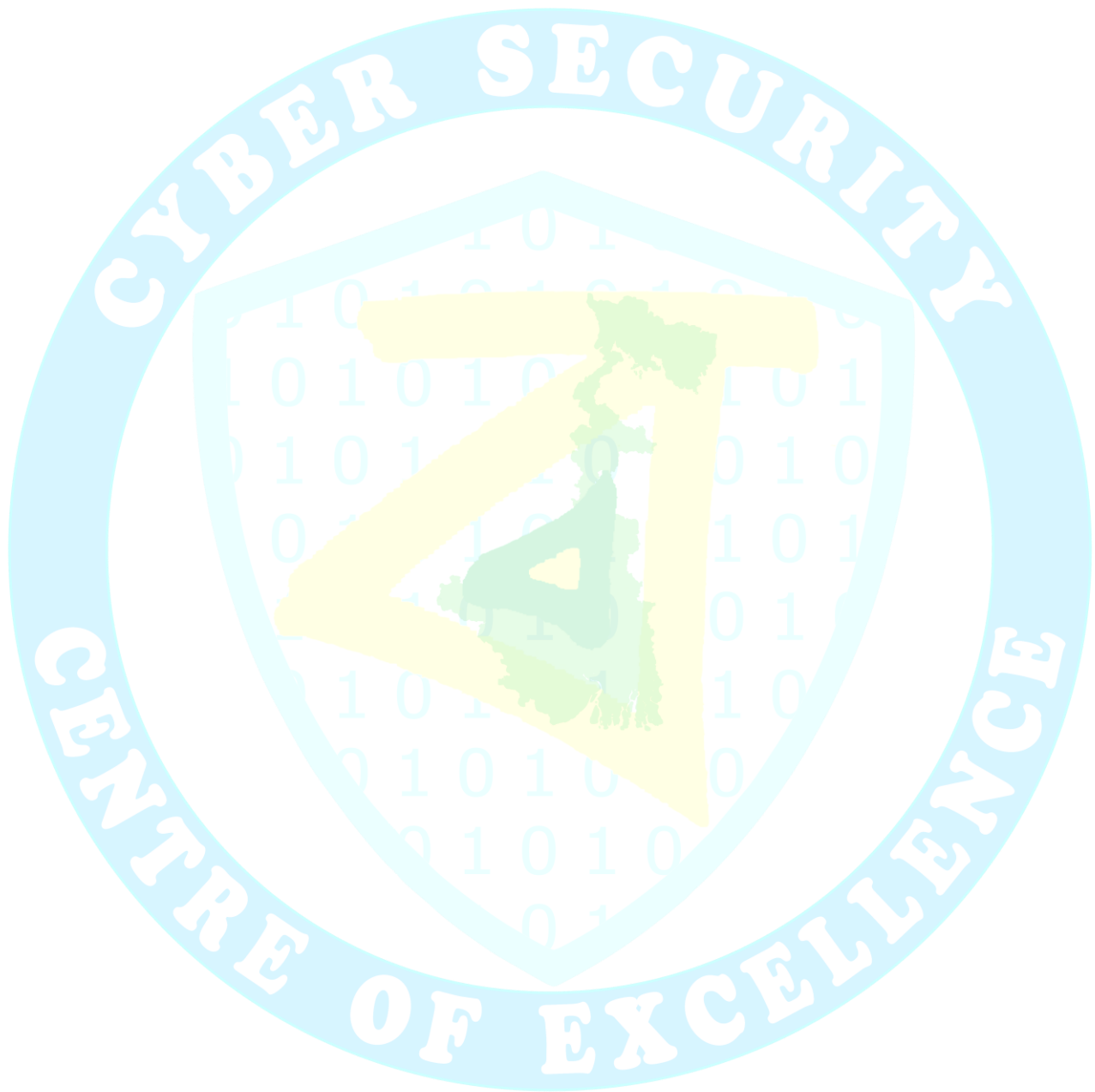
CYBER SAFE BENGAL



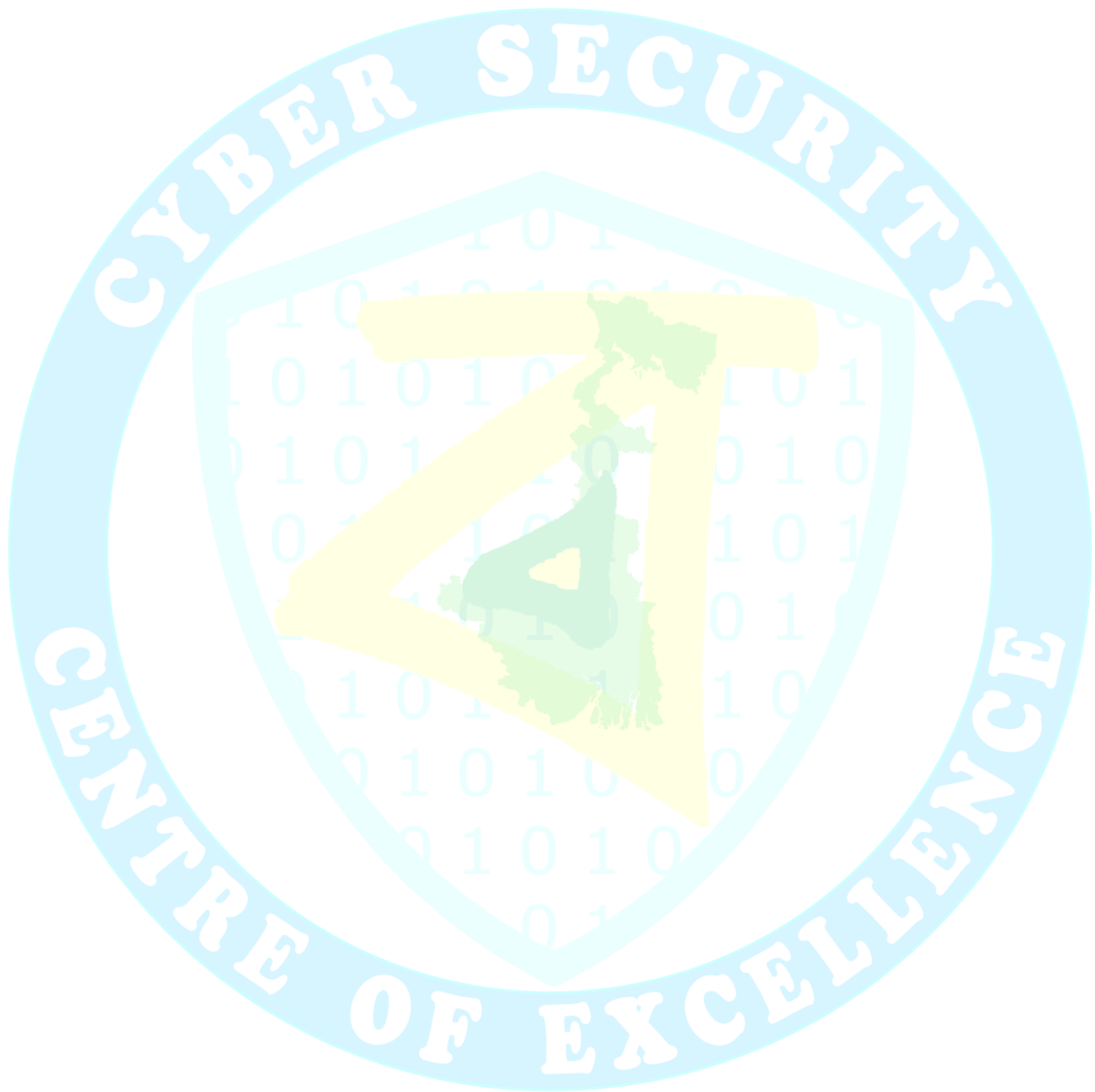
CYBER SAFE BENGAL



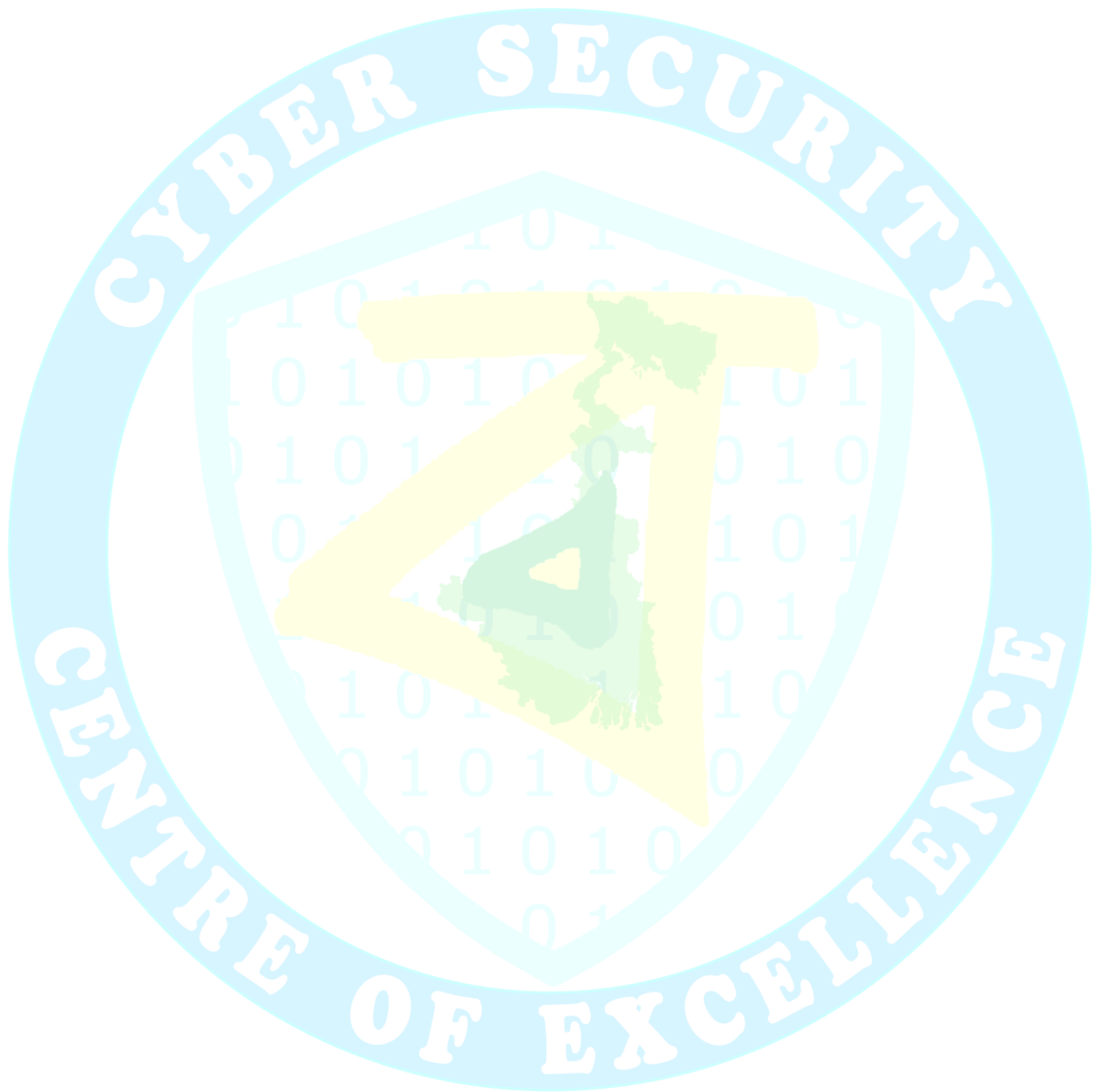
CYBER SAFE BENGAL



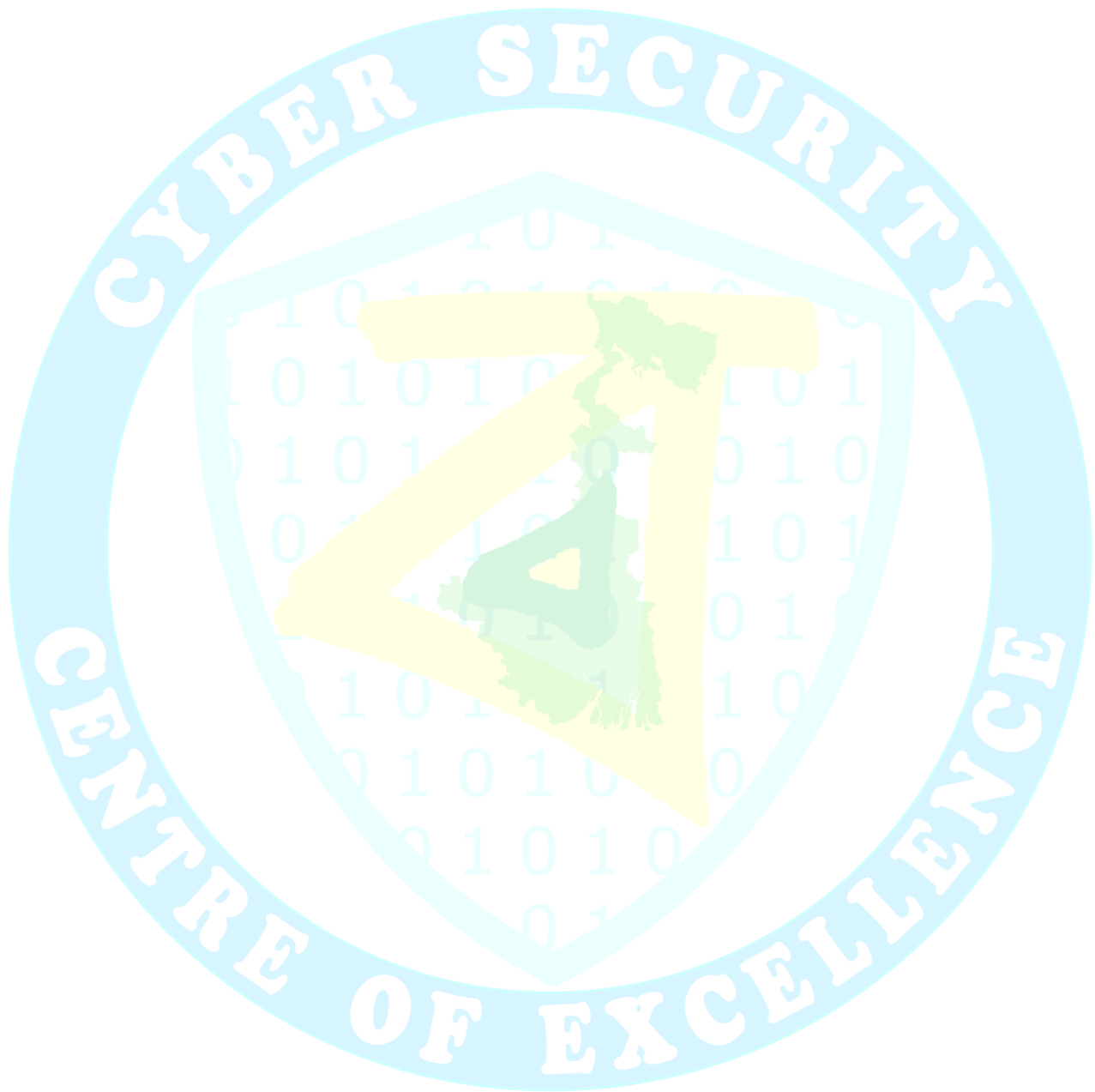
CYBER SAFE BENGAL



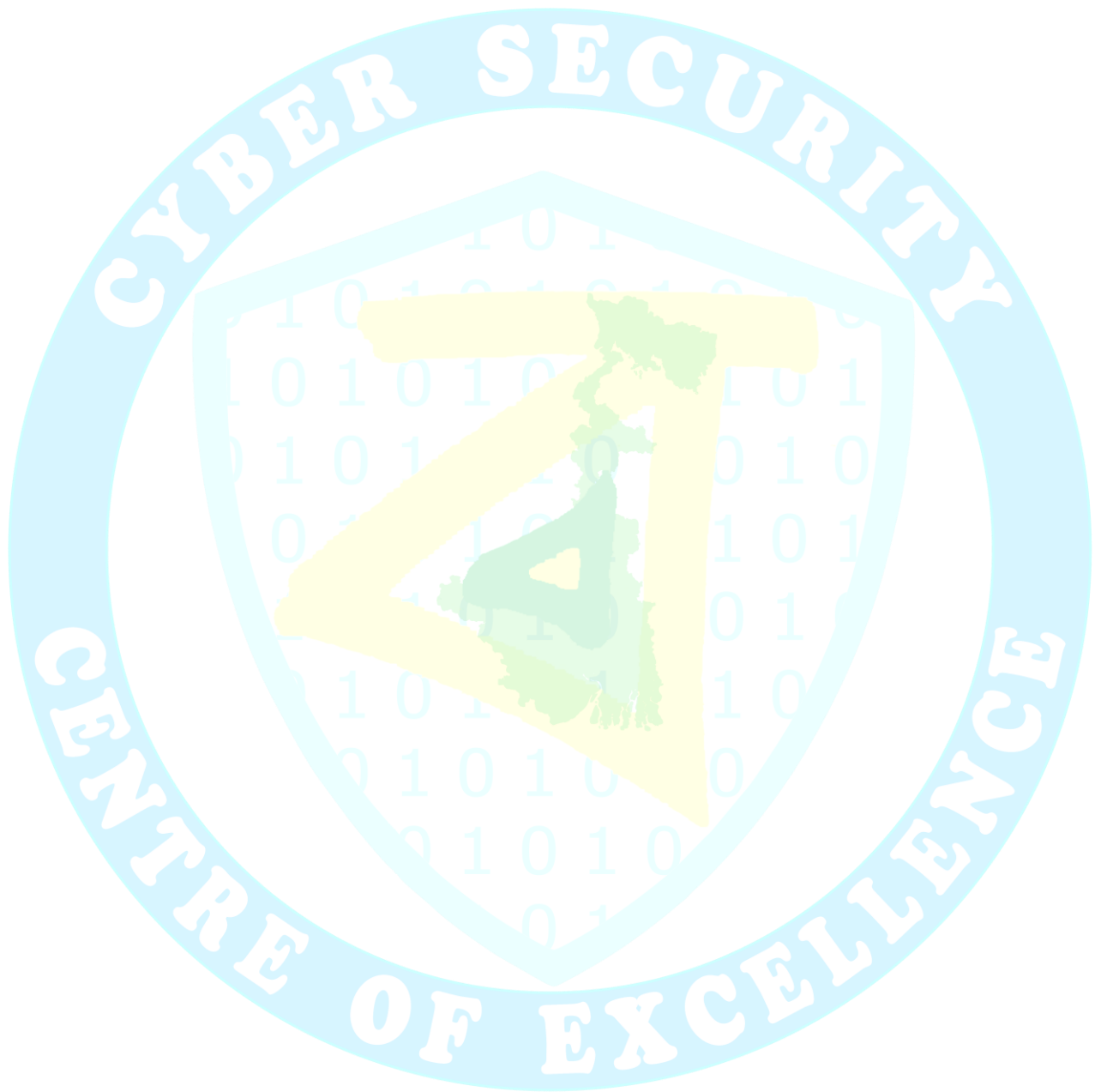
CYBER SAFE BENGAL



CYBER SAFE BENGAL



CYBER SAFE BENGAL



CYBER SAFE BENGAL
