DIGITAL BANGLADESH
Skilled. Equipped. DigitalReady.

ICT DIVISION
FUTURE IS HERE

DIGITAL SECURITY AGENCY

BGD e-GOV CIRT

BANGLADESH CYBER SECURITY STRATEGY 2021 - 2025

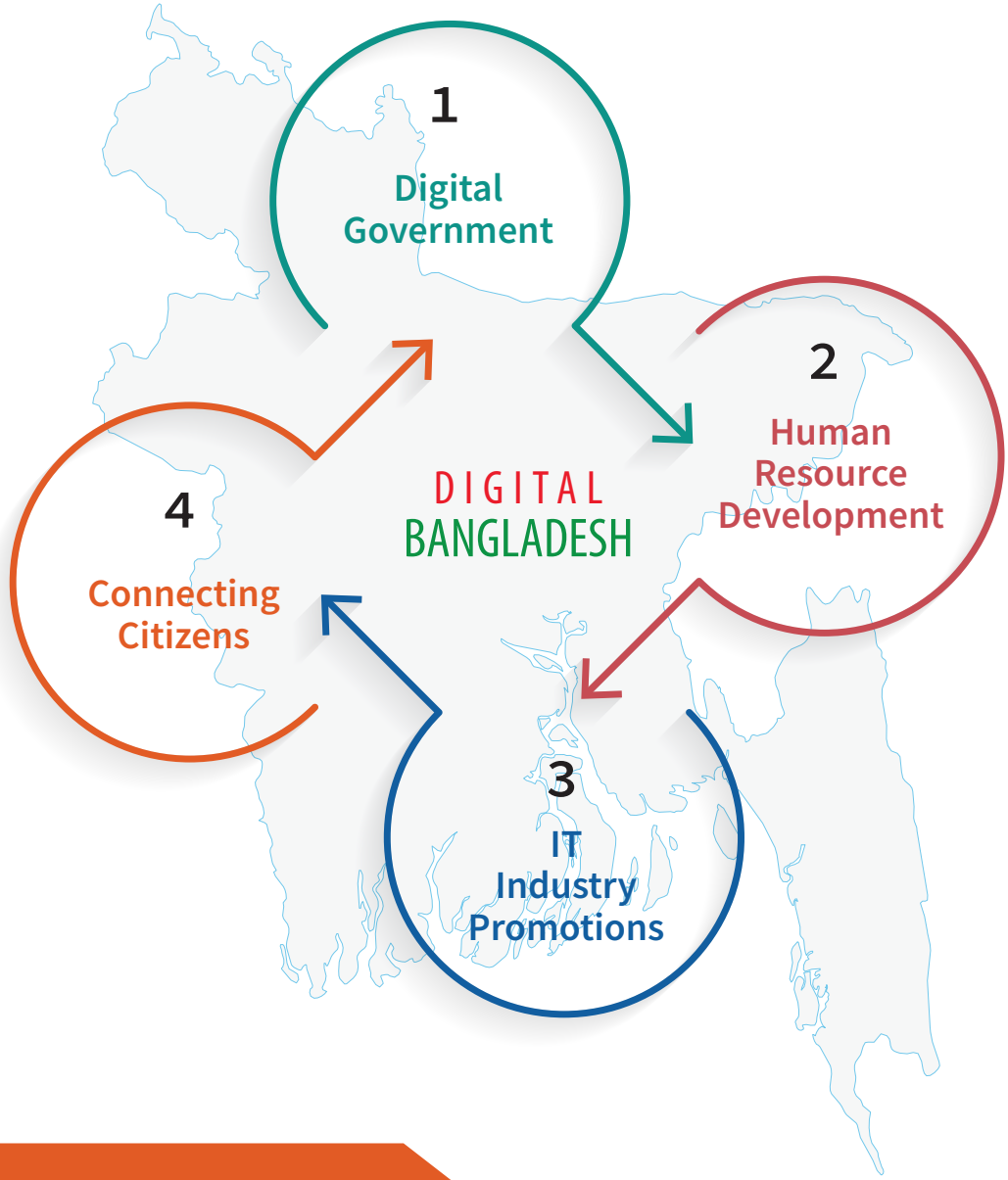
WE ARE

N-CERT

OF BANGLADESH

CONTENTS TABLE

PILLARS OF DIGITAL BANGLADESH



Enhancing National Cyber Security Governance and Ecosystem

01

To strengthen governance and ecosystem in cyber security

02

To enhance collaboration and building trust among government agencies, CII agencies, businesses and partners through information sharing and effective Public-Private Partnership

03

To establish and implement National Communication Mechanism for effective coordination, information sharing and media management

Improving Organization Management and Business Operation (Government, CII and Business)

04 To adapt cyber security in business operation

05 To enhance holistic cyber security controls in supply chain environment

06 To comply with International Standard (Information Security Management Systems, Business Continuity Management Systems or equivalent) and Best Practices

07 To promote the use of certified ICT security products

08 To implement Secure Software Development Life Cycle (S-SDLC) for critical Information System Development

Improving Organization Management and Business Operation (Government, CII and Business)

09 To establish Data Leakage Protection Mechanism

10 Adoption and Certification of ICT system such as ISO/BDS, PCI-DSS, CMMI, TMMI, Uptime etc.

11 To develop Vulnerability Assessment and Penetration Testing (VAPT) Implementation Plan and conduct periodic risk assessment and VAPT on all critical ICT services

12 To measure National Readiness Level through periodical study

13 To enhance Industrial Control System (ICS) Protection

14 Mandatory external IT System Audit and submission of IT System Audit report to Digital Security Agency (DSA) for all CIIs on yearly basis

Strengthening Cyber Security Incident Management and Active Cyber Defense

15 To strengthen capacity and capability in Incident Management through establishment of National Security Operation Center (N-SOC)

16 To develop capacity in combating terrorist/extremist use of Internet

17 To enhance national readiness towards bigger scale and targeted cyber attacks

HUMAN RESOURCE DEVELOPMENT

STRATEGY # 04-06

Enhancing National Cyber Security Capacity and Capability Building

01

To develop National Cyber Security Capacity and Capability Building Plan

Enhancing National Cyber Security Capacity and Capability Building

02

To develop a comprehensive plan to build adequate tools and technology through an integrated approach

Nourishing Cyber Security Knowledge Through Education

03

To develop cyber security subject as one of the syllabi at the primary, secondary and tertiary level through collaboration with Ministry of Education, University Grant Commission (UGC)

Enhancing Cyber Security Awareness

04

To improve cyber security awareness program implementation approach through adoption and implementation of the National Cyber Security Awareness Master Plan

Spurring National Cyber Security R&D Program

01 To stimulate and encourage cross discipline research and collaboration

Promoting a Competitive Local Industry and echnology

02 To stimulate the creation of new local cyber security ventures through the establishment of cyber security start-up / incubation hub

03 Promote the use of local ICT security products and services and support the growth and expansion of the local cyber security industry

04 To strengthen academic centers of excellence in universities through collaboration with academia, educational institutes and industry

Enhancing Bangladesh's Cyber Laws to Address Current and Emerging Threats

01

To enhance and review current legal frameworks to address cybercrime

02

To study the need to introduce a new laws, i.e.

- Data Protection Act
- Digital Security Act
- Act/ Strategy/ Policy for Emerging Technologies (Big Data, Machine Learning, Artificial Intelligence, Block chain, IoT etc.)
- Appropriate rules under the acts.
- Appropriate guidelines and frameworks for the application of the acts.

Enhancing the Capacity and Capability of Cybercrime Enforcement

03

- To strengthen cybercrime enforcement capacity and capability in managing cybercrime, advanced threats and organized syndicates
- Training of Judiciary for prosecution under laws related to cyber crime
- Training of law enforcement personnel.
- Investment in startups to promote local cyber security companies.
- Investment in the education system for producing **250+**
- Bachelors, **100+** Masters and **25+** PhD in Cyber Security from Public Universities.
- Introduction of local cyber security index to award best achievers.
- Establishment of Cyber Gym in all universities offering Computer Science (CS), Computer Science & Engineering (CSE) and Cyber Security.

Pillars of Digital Bangladesh

Pillars # 1

DIGITAL GOVERNMENT

Digital Bangladesh vision has brought the services to the doorsteps of citizens through fast digitization and e-service rollout. Now government intends to consolidate and secure these services in the cyberspace. The focus is now on strengthening the four pillars of Digital Bangladesh in cyberspace. In an ideal world, we would have a national standard for governance and management that allows for shared accountability and cross-sectional integration to maximize efforts in responding to concerns, threats, and breaches.

An active cyber defense posture, ranging from Advanced Persistent Threat to cybercrime and content-related challenges, is required to increase national resilience against cyber threats. To reduce cyber risks, this strategy will promote both defensive and offensive capabilities, with an emphasis on the capacity to detect, analyze, and respond to any cyber threat inside our ICT ecosystem.

Digital Security Agency will enforce a sustainable governance and management structure to support the duties assigned to it through Digital Security Act 2018. The governance and communication will be dynamic, adaptable, and ready to meet the challenges to attain better resilience. It should provide effective framework for action plans, promoting strong partnerships among stakeholders such as Critical Information Infrastructures (CIIs), law enforcement agencies, organizations, general public etc. These collaborations will provide platforms for exchanging information, developing strategies, and pooling of the resources.

This will help to realize secured Digital Bangladesh through supporting three major objectives:

- Improving the secured governance and ecosystem for Digital Bangladesh;
- Improving the government's, CII's, and enterprises' organizational management and business operations;
- Increasing the effectiveness of cyber security incident response and cyber defense;

DIGITAL GOVERNMENT

The Pillar-I (Digital Governance) aims at enhancing the capacity to defend organizational networks, data, and systems from cyber-attacks and mitigation of threats. Organizations will invest to improve capacity to predict, identify, investigate and mitigate threats. The organization will adopt ITIL (Information Technology Infrastructure Library)/ ISO/BDS standards clearly outlining the duties and responsibilities of all stakeholders within the ecosystem in order to improve the national cyber security governance framework. Threat information sharing platforms will coordinate with Digital Security Agency (DSA) to identify and close gaps in responsibility and coordination across agencies.

DSA will serve as the focal point for the execution of proactive measures to secure the government and CIIs networks, systems, and data, as well as to strengthen inter-agency collaboration in the fight against cybercrime. However, individual CIIs and institutions will be solely responsible for ensuring security of their own ICT infrastructures and applications. Outsourcing or delegating security obligations to a third party will not relieve or indemnify organizations of their security obligations.

All Security Operation Centers (SOCs) in Bangladesh will report to the N-CERT for coordination among SOCs.

Digital Bangladesh has contributed to the rise of e-government initiatives, e-commerce transactions, and digital economy. This had made inroads in the usage of Artificial Intelligence and machine learning in modern systems, the increasing application of IoT in devices and peripherals, 5G communication systems and the extensive use of complex Industrial Control Systems. All of which inadvertently would open up even more avenue for potentials risks and threats to security, safety and privacy. Specially, the production at industries will be dependent on 5G communications for production controls. These have the potential to stop critical operations through back doors available on such platforms. Appropriate policies and guidelines for usage of 5G in production and control systems will be formulated for security and privacy.

Government-led Technical Working Group will be established to spearhead an in depth study on laws, rules and regulations as well as standards and best practices in cyber security that have to be adhered to for adaption of 5G and other 4IR technologies in the country. A training platform to assist participating organizations in complying with cyber security standards will be established. Data Protection Act and Rules will be enacted to protect data leakage protection mechanism through proper policies, procedures and guidelines related to data protection, public key infrastructure (PKI) and electronic information management.

Pillars of Digital Bangladesh

Pillars # 1

DIGITAL GOVERNMENT

Computer Emergency Response Teams (CERTs) will be established and registered by DSA in all CIIs to improve and strengthen the National Cyber Security Incident Response Team (CSIRT), Sector CSIRT and Organization CSIRT. The CSIRTs will be provided with the necessary capabilities and capacity to handle, mitigate and recover from cyber crisis and incidents. Cyber incident reporting to DSA is mandatory for all organizations and CIIs as per the Digital Security Act, 2018. IT System Audit, Vulnerability Assessment must be conducted on yearly basis and reported to DSA.

Combating terrorists and violent extremists' use of the Internet will continue to be a priority area, with the main objectives of: raising awareness among the public; and preventing radicalization and terrorist recruitment and fund raising activities through digital platforms such as social media and web portals. An integrated information-sharing platform shall be developed to facilitate flow of information between relevant agencies.

The implementation of the Bangladesh Cyber Security Strategy will be supervised through an annual evaluation process, after which a Bangladesh Cyber Security Strategy landscape report will be prepared and presented to the stakeholders for milestone reviews and further deliberations.

STRATEGIES

01

Enhancing National Cyber Security Governance and Ecosystem

- To strengthen governance and ecosystem in cyber security
- To enhance collaboration and building trust among government agencies, CII agencies, businesses and partners through information sharing and effective Public-Private Partnership
- To establish and implement National Communication Mechanism for effective coordination, information sharing and media management

02

Improving Organization Management and Business Operation (Government, CII and Business)

- To adapt cyber security in business operation
- To enhance holistic cyber security controls in supply chain environment
- To comply with International Standard (Information Security Management Systems, Business Continuity Management Systems or equivalent) and Best Practices
- To promote the use of certified ICT security products
- To implement Secure Software Development Life Cycle (S-SDLC) for critical Information System Development
- To establish Data Leakage Protection Mechanism

DIGITAL GOVERNMENT

STRATEGIES

02

Improving Organization Management and Business Operation (Government, CII and Business)

- Adoption and Certification of ICT system such as ISO/BDS, PCI-DSS, CMMI, TMMI, Uptime etc.
- To develop Vulnerability Assessment and Penetration Testing (VAPT) Implementation Plan and conduct periodic risk assessment and VAPT on all critical ICT services
- To measure National Readiness Level through periodical study
- To enhance Industrial Control System (ICS) Protection
- Mandatory external IT System Audit and submission of IT System Audit report to Digital Security Agency (DSA) for all CIIs on yearly basis.
- To strengthen capacity and capability in Incident Management through establishment of National Security Operation Center (N-SOC) To develop capacity in combating terrorist/extremist use of Internet
- To enhance national readiness towards bigger scale and targeted cyber attacks

03

Strengthening Cyber Security Incident Management and Active Cyber Defence

- To develop National Cyber Security Capacity and Capability Building Plan
- To develop a comprehensive plan to build adequate tools and technology through an integrated approach
- To improve cyber security awareness program implementation approach through adoption and implementation of the National Cyber Security Awareness Master Plan
- To develop cyber security subject as one of the syllabi at the primary, secondary and tertiary level through collaboration with Ministry of Education, University Grant Commission (UGC).

HUMAN RESOURCE DEVELOPMENT

To meet the challenges of the rapidly changing nature of cyber threats, the government will develop and implement a comprehensive National Cyber Security Capacity and Capability Plan that will determine the areas of expertise and skill sets that will need to be continuously improved and enhanced at national, sectoral and organizational levels.

Correspondingly, this Pillar aims to enhance capacity and capability building, awareness and education through three strategic initiatives, specifically by:

- Enhancing national cyber security capacity and capability
- Enhancing cyber security awareness
- Nourishing cyber security knowledge through education

The Plan will be implemented by building coherent cross sector collaboration in strategic information sharing and security awareness initiatives, deepening the understanding of advanced threats, developing a culture that understands security risks in the context of business resiliency and expanding the capability to develop a safer and more resilient technology, as well as the ability to respond to advanced threats.

Bangladesh has been developing and implementing cyber security capacity and capability through various ministries, agencies and CII organizations. Enhancements of national cyber security capacity and capability will be focused on increasing the number of local skilled professionals through training and certification programs to meet the demands for skilled workforce in both the public and private sectors. Specialist skill development, on the other hand, requires pursuing good quality and established security professional certifications primarily in specific areas of cyber security domain, that are lacking in the country.

Meanwhile, awareness and education would require, among other things, the identification of necessary target audiences and content development approaches that can enable resource sharing and collaboration. The government, through its various agencies, will take up the crucial role of empowering all levels of society to understand cyber security-related risks and challenges, as well as the necessary defensive measures needed for safer Internet use.

The government will also provide additional funding and scholarships in order to encourage knowledge acquisition and enrichment among existing cyber security professionals. This will help develop a new generation of cyber security professionals, with necessary education and skills.

Currently, Bangladesh Government has started its efforts to increase the number of local cyber security professionals through the implementation of Global Accredited Cybersecurity Education (ACE) Scheme. It is a holistic professional certification scheme established indigenously to certify and recognize cyber security personnel in tandem with ISO/IEC 17024 on people certifications, ISO/IEC 9000 on processes and ISO/IEC 27001 on security management.

To enhance Bangladesh's approach on cyber security awareness, the government will develop and implement the National Cyber Security Awareness Master Plan. Under the Plan, the National Cyber Security Awareness Governance structure will be established, which aims to develop an integrated and concerted cyber security awareness program. The primary aim of the integrated program is to reduce the number of cyber incidents by running cyber security awareness programs and call for actions that are more organized, coordinated and able to reach a wider target audience among Bangladeshi.

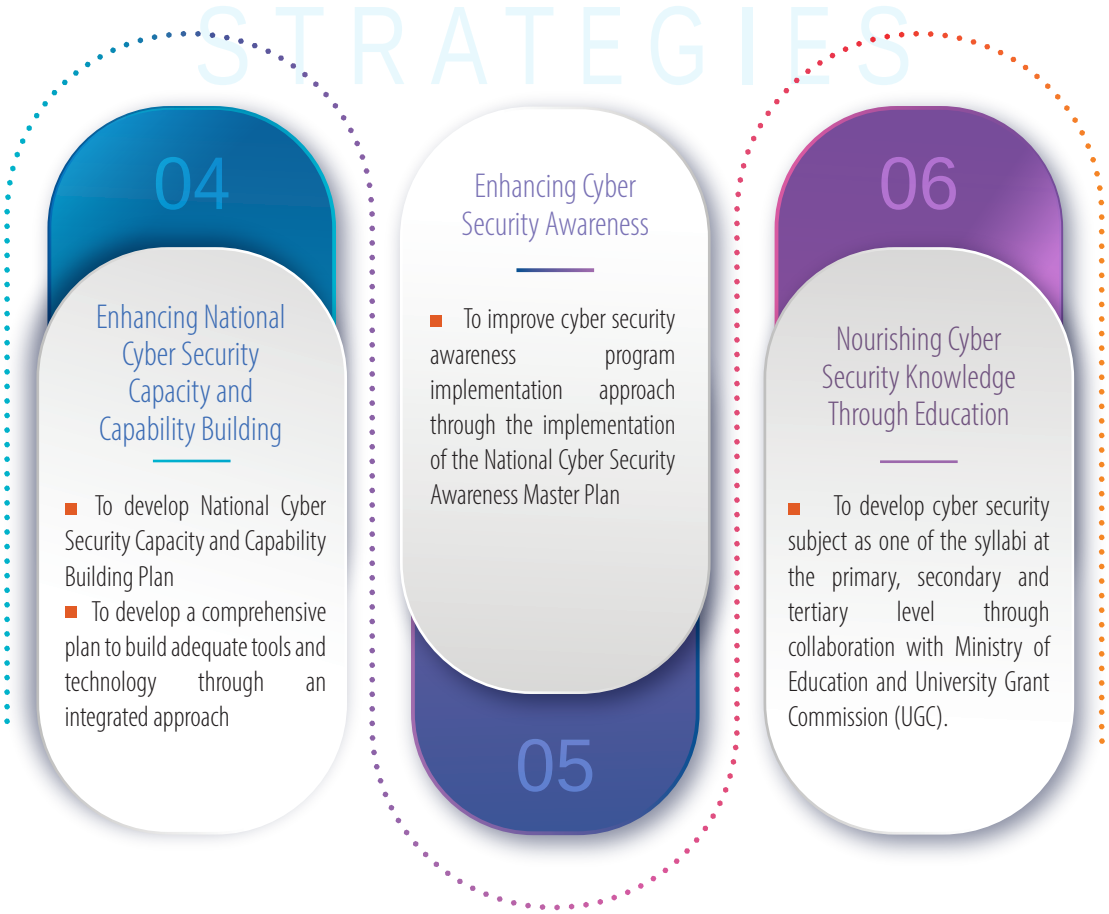
The Plan will outline integrated initiatives on public-private driven collaboration and coordination, and the mobilization of resources to enable a wider outreach of programs to kids, youth, adults/parents and organizations. Initiatives by various agencies will also be implemented in an integrated and coordinated manner to ensure a wider coverage and bigger impact. This will be crucial in educating citizens on the necessary knowledge to detect and avoid abuse, fraud and crime online, as well as to nurture accountable behavior, thereby creating well-informed and responsible cyber citizens.

At the same time, we will also be working on establishing a creative content development program mechanism that brings together all the stakeholders, from both the public and private sectors, to share their experience and best practices on creating awareness. It is hoped that a unified national brand of cyber security awareness program can then be developed, one which streamlines the content of various awareness programs based on the accepted security baseline framework. A corresponding measurement mechanism will also be appropriately devised to evaluate the effectiveness of the said programs and to identify ways to improve them from time to time.

Cyber security will also become part of the syllabi at the primary, secondary and tertiary level of education. Given the increasing threats from cyberspace and the all-embracing nature of ICT and the Internet, especially among the younger generation of Bangladeshi, we believe that it is never too early to introduce and foster cyber security awareness. Our youth needs to be equipped with the necessary cyber security knowledge and tools to ensure safety and security.

In academia, there is a need to embed cyber security across taught courses under ICT and Computer Engineering programs. As an example, cyber security requirements need to be taught in Software Programming (secure coding), Software and System Development Cycle (Secure SDLC), Database, Operating Systems, Network, IT Administration and Management, as well as cross platform application development. This effort is in addition to the present dedicated cyber security related courses being taught in colleges and universities.

The same effort of introducing cyber security related issues across non-ICT or non-Engineering disciplines covering cyber law in Law, FinTech in Finance, security risk management of network ready medical devices in Health, among others, is necessary to enable graduates to stay relevant and to be able to grasp the impact of new technological developments. Within the Public Service Department, there is a need to establish cyber security as a vertical (grade) in the government sector to enable specialization in the various domains under information security and to enable retention of these trained personnel within their expertise by providing sufficient opportunities for career growth.



IT INDUSTRY PROMOTIONS

07 Spurring National Cyber Security R&D Program

- To stimulate and encourage cross discipline research and collaboration

08 Promoting a Competitive Local Industry and Technology

- To stimulate the creation of new local cyber security ventures through the establishment of cyber security start-up / ideation hub
- To promote the use of local ICT security products and services and support the growth and expansion of the local cyber security industry
- To strengthen academic centres of excellence in universities through collaboration with academia, educational institutes and industry

Pillars # 4

CONNECTING CITIZENS

Digital connectivity has both empowered and endangered businesses and individuals. It opens new social and commercial opportunities, yet also exposes citizens to criminal syndicates across the world. By commandeering computing devices, these malicious actors can steal data; extort money, and attack networks, causing harm to others. Cyberspace needs to be kept safe and trustworthy for businesses and individuals to benefit from it. Keeping cyberspace safe requires a spectrum of actions from the international to individual levels. Countries have to cooperate to take down criminals operating across borders, while businesses and individuals can take preventive measures to keep their systems and devices safe. Cybersecurity is the collective responsibility of everyone - the Government, businesses, individuals and the community.

Working together, the administrative branches and the business community will chart the legislation, including any needs to review the provisions relevant to the cyber domain and cyber security. The results of this action will comprise the proposals for legislative review which will advance the achievement of the goals of the Cybersecurity Strategy.

The charting will take into account the rapidly changing phenomena in the cyber domain. One of the purposes is to provide the competent authorities and other actors with the sufficient means and powers through legislation to implement cyber defenses for the functions vital to society and, especially, the security of the state. Any possible legislative hurdles, restrictions and obligations related to data protection, as well as those arising from international obligations, that impede the obtainability, disclosure and exchange of information useful for effective cyber defense purposes, will be taken under review. When it comes to the assessment of information-gathering and other data processing one should also estimate whether the competent authorities should have improved possibilities for gathering information, data processing, or being informed of cyber threats and their sources, while simultaneously paying attention to ensuring the basic rights of privacy and confidentiality in electronic communications.

Pillars of Digital Bangladesh

Pillars # 4

CONNECTING CITIZENS

09 Enhancing Bangladesh's Cyber Laws to Address Current and Emerging Threats

- To enhance and review the current legal frameworks to address cybercrime
- To study the need to introduce a new laws, i.e
  - Data Protection Act
  - Digital Security Act
  - Act/ Strategy/ Policy for Emerging Technologies (Big Data, Machine Learning, Artificial Intelligence, Block chain, IoT etc.)
  - Appropriate rules under the acts.
  - Appropriate guidelines and frameworks for the application for the acts.

10 Enhancing the Capacity and Capability of Cybercrime Enforcement

- To strengthen cybercrime enforcement capacity and capability in managing cyber-crime, advanced threats and organized syndicates
  - Training of Judiciary for prosecution under laws related to cyber crime.
  - Training of law enforcement personnel.
  - Investment in startups to promote local cyber security companies.
  - Investment in the education system for producing 250+ Bachelors, 100+ Masters and 25+ PhD in Cyber Security from Public Universities.
  - Introduction of local cyber security index to award best achievers.
  - Establishment of Cyber Gym in all universities offering Computer Science (CS), Computer Science & Engineering (CSE) and Cyber Security.

The notion of digital society reflects the results of the modern society in adopting and integrating information and communication technologies at home, work, education and recreation. Digital innovations are reshaping our society, economy and industries with a scale and speed like never before. Mobile and cloud technologies, Big Data and the Internet of Things offer unimaginable opportunities, driving growth, improvement of citizens' lives and efficiency to many areas including health services, transportation, energy, agriculture, manufacturing, retail and public administration.

All the aforementioned digital innovations need to be implemented with trust and security. In the digital world, cybersecurity is a prerequisite for the safety of individuals, society and the economy. Innovation will be the key for cybersecurity in order for Bangladesh to be at the forefront of global competition. Our policies must prioritize cybersecurity and ensure security-by-design across three pillars: people, process and technology. Policies must protect the citizens' right to safety, security and privacy; support businesses in innovation; and enable law enforcement to use digital resources to protect public security online and offline in ways which do not undermine public trust in technology. Compliance with modern and harmonized personal data protection rules; with well- established standards of security-by-design in all digital technologies, networks and services; and clear privacy rules that balance citizens' rights and businesses' needs, are vital for building trust and security. The regulatory framework should be guided by the concept of «as little as possible and as much as necessary», fit for the digital age, and open and technologically neutral enough to accommodate future developments.

Strategic Objectives

- To build security and trust in an open and free digital society.
- To strengthen the security of digital society in order to give individuals, businesses, and public bodies more confidence in the use of ICT.
- To ensure legal protection in the digital domain, prevent social disruption, and lead to appropriate action if things go wrong.

To achieve these strategic objectives, the following lines of action have been drawn up:

- Facilitate Digital identity for every citizen so that everyone can use simple and secure digital credentials.
- Identify and prevent vulnerabilities and handle incidents. This requires awareness of information and cybersecurity and of how to protect information systems.
- Ensure privacy in the digital society. The use of personal data is often crucial to streamline and develop both public and the private services. The right to privacy is essential to maintain confidence, security and trust in the digital environment.
- Preserve democracy in digital environments. Opportunities to spread threats, hatred, extremist propaganda and deliberate dissemination of false information increase. Freedom of expression must be given very wide limits. However, strong action is required against criminal acts in digital environments.
- Foster a secure and mobile labour market. Digitalization fundamentally changes the labour market, including the nature of the work and working environment. Close dialogue between the government and social partners to ensure continuous adaptation to social development is essential.
- Promote well functioning digital markets and secure consumers. Digital markets must always be a safe and legal place for consumers and businesses. Regulatory and supervisory authorities should maintain effective consumer protection and competition on equal terms.

DIGITAL BANGLADESH
Skilled, Equipped, DigitalReady.

ICT DIVISION
FUTURE IS HERE

DIGITAL SECURITY AGENCY

BGD e-GOV CIRT

BANGLADESH CYBER SECURITY STRATEGY 2021-2025