



# Data Security Policy of BIGM 2024

**Bangladesh Institute of Governance and Management (BIGM)**


A handwritten signature in black ink, appearing to read "Krishna Gayen", is written over the printed name.

**Dr. Krishna Gayen**  
Sr. Research Fellow  
Bangladesh Institute of  
Governance & Management

A handwritten signature in black ink, appearing to read "Mohammad Tareque", is written over the printed name.

**Dr. Mohammad Tareque**  
Director  
Bangladesh Institute of  
Governance and Management (BIGM)

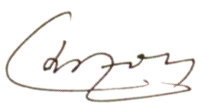
  
**Dr. Krishna Gayen**  
Sr. Research Fellow  
Bangladesh Institute of  
Governance & Management

  
**Dr. Mohammad Tareque**  
Director  
Bangladesh Institute of  
Governance and Management (BIGM)

## Abbreviation

- **CPU** - Central Processing Unit
- **ACL** - Access Control List
- **ACEs** - Access Control Entries
- **VPN** - Virtual Private Network
- **RBAC** - Role-Based Access Control
- **VLAN** - Virtual LAN
- **ERP** - Enterprise Resource Planning (ERP)
- **DMZ** - De-militarized Zone
- **Wi-Fi**- Wireless Fidelity
- **TCP** - Transmission Control Protocol
- **SSH** - Secure Socket Shell
- **LAN** - Local Area Network


  
**Dr. Krishna Gayen**  
Sr. Research Fellow  
Bangladesh Institute of  
Governance & Management

  
**Dr. Mohammad Tareque**  
Director  
Bangladesh Institute of  
Governance and Management (BIGM)

## Tables of Contents

Abbreviation.....	iii
1. Preamble.....	1
2. Purpose.....	1
3. Scope.....	1
4. Security Principle.....	2
5. Policy.....	2
5.1 User Security and Access Guidelines.....	2
5.2 Server Access Policy.....	4
5.3 Network Access Policy.....	5
5.4 Enterprise Resource Planning (ERP) Access Policy.....	6
5.5 Application Access Policy.....	8
5.6 Other Policies.....	9
6. Reporting Requirements.....	10
Annex-I.....	A

  
**Dr. Krishna Gayen**  
Sr. Research Fellow  
Bangladesh Institute of  
Governance & Management

  
**Dr. Mohammad Tareque**  
Director  
Bangladesh Institute of  
Governance and Management (BIGM)

# DATA SECURITY POLICY OF BIGM 2024

## 1. Preamble

Bangladesh Institute of Governance and Management (BIGM), formerly known as Civil Service College, Dhaka, a post-graduate institute affiliated to University of Dhaka, has been established in 2006 to create a premium knowledge hub of international standard for studies, research and high-level skills training on public policy, management, and promotion of good governance in the country.

BIGM conducts academic, research, and training programs. A large number of research articles have been published in peer-reviewed journals, and many research works are ongoing and many are under review. The institute offers training programs in 2 domains: Governance and Research. Policy Analysis, Strategic Management, Specialized Procurement Training, VAT Management, and Advance Project Management courses are offered in the Governance domain, and Quantitative Analysis with STATA, Fundamentals of Research Methodology, Data Analytics in R and Python and Machine Learning courses are offered in the Research domain.

In addition, BIGM also conducts Master's in Public Affairs (MPA) programs in six areas: Governance and Public Policy (GPP), International Economic Relations (IER), Human Resource Management (HRM), Project Management (PM), Procurement and Supply Chain Management (PSCM), Public and Private Financial Management (PPFM). BIGM requires to keep a record of the information regarding its students, faculties, and staff, which include the following:

- i. the enrollment of students
- ii. the recruitment, employment, and payment of staff
- iii. proper administration of courses and assessment of student assignments and performance
- iv. student welfare
- v. redesigning the courses

## 2. Purpose

The purpose of this policy is to set out the standards for the base configuration, and acceptable use of any software, hardware and network owned and/or operated by BIGM. Effective implementation of this policy will reduce the risks associated with the theft, loss, misuse, damage and abuse of the assets. This policy is for ensuring that BIGM's authorized user understand their own responsibilities for protecting, preserving and managing the confidentiality, integrity and availability of BIGM's data.

## 3. Scope

This data security policy:

- I. Applies to all BIGM's officers, faculties, and staff irrespective of their state of contract (full-time, part-time) as well as the members of the wider BIGM Family.
- II. Covers all data handled, stored, processed or shared by BIGM, irrespective of whether that information originates with or is owned by BIGM.
- III. Applies to all computer and non-computer based information systems owned by BIGM or used for BIGM.
- IV. BIGM's data can broadly be classified as **personal data** and **non-personal data**.

- **Personal data** is treated in accordance with BIGM’s Data Protection Policy and is afforded the highest standard of protection.
- **Non-personal data** can include:
  - a. Sensitive organizational data such as commercially sensitive planning data, research data, data protected by confidentiality agreements or legally privileged information – all of these categories of data are also afforded a high level of protection.
  - b. Other organizational data that is either already made public (e.g. on the BIGM website) or is potentially dis-closable to the public (e.g. that which may be requested under the Freedom of Information request) – such data must be accurate, must be kept up-to-date and must be protected from destruction and unauthorized interference.

#### 4. Security Principle

- I. **Data safety:** This category refers to basic data protection measures enforced for decades. BIGM must create data backups and enforce data retention processes.
- II. **Data security:** This category involves securing data flows with the best encryption protocols while ensuring strong authentication processes are in place. BIGM must also implement threat monitoring solutions for faster incident response times.
- III. **Data privacy:** This category addresses third-party Access to data. BIGM must continuously monitor and document all data outside their ecosystem.
- IV. **Lawfulness:** All data processing must have a legal basis, such as website performance-related data, and can start only after a user consents.
- V. **Transparency:** Fairness covers all data collection, while transparency server’s data sharing and processing procedures. Because BIGM works with so many applications and research papers, communicate these connections and dependencies in written form to ensure transparency while minimizing "invisible processing" procedures.
- VI. **Accuracy:** Keep data as accurate as possible. In addition, users must be able to fix inaccurate data, known as the right to rectification.
- VII. **Integrity and confidentiality:** Minimize accidental data leaks by taking appropriate technical and organizational steps, including ongoing security training for existing and new employees. It must ensure that the IT Department has appropriate security measures to protect the BIGM officials' data.
- VIII. **Accountability:** As the data controller, BIGM is responsible for data protection. Document all data collection and processing activities to demonstrate compliance.

#### 5. Policy

The policy's provisions, which constitute its body, are stated in this section. BIGM shall make all necessary information available to all employees and contracted third parties so that they may carry out their duties as effectively and efficiently as feasible.

##### 5.1 User Security and Access Guidelines

###### i. Password Security:

Users must use strong passwords with a minimum length of 12 characters, including a combination of upper and lowercase letters, numbers, and special symbols (e.g., @Aa123456\_@#^12).



- ii. **Internet Access Permissions:**  
Restrict access to Facebook, YouTube, job sites, and social media on user PCs. Obtain permission from the Wing Chief of the Strategic Planning Wing and notify the IT team for access approval.
- iii. **Data Access Permissions:**  
Users may access data in their wing-wise common shared folder. Seek IT team approval for access to other shared folders.
- iv. **Antivirus Protection:**  
Keep antivirus software up-to-date. Scan pen drives or external drives with antivirus before use. Conduct weekly antivirus scans on computers and report any concerns to the IT team promptly.
- v. **Email Usage:**  
Use the official email strictly for office work; personal use is prohibited.
- vi. **Data Handling:**  
Upload official work data to Google Drive and maintain a folder on the computer drive. Share important data through Google Drive. If anyone share data from the common folder for a particular purpose, he\she should delete it after completion of work.
- vii. **External Storage and Desktop Usage:**  
Do not directly work on pen drives or external hard drives with official data. Avoid working from desktop files; store all files inside the drive to prevent data loss.
- viii. **Computer Security:**  
Lock the screen when leaving the computer.
- ix. **Email Security:**  
Exercise caution with unknown emails; do not click links or download files from unknown emails.
- x. **Media Usage Policy:**  
Prohibit watching videos, movies, or social media during office hours. Violators may face disciplinary action based on IT TEAM log evidence.
- xi. **Software and Large Downloads:**  
Inform IT TEAM in advance for large software or video downloads to avoid disruptions for other users.
- xii. **Training and Awareness Programs**  
BIGM is committed to maintaining a vigilant and informed user community. To achieve this, regular training sessions and awareness programs will be conducted for all employees and contracted third parties. These programs will cover essential topics such as password security, recognizing phishing attempts, and best practices for data handling. The goal is to empower users with the knowledge and skills necessary to contribute to the overall security posture of BIGM.
- xiii. **Incident Response Team Contact Information**  
In the event of a security incident or breach, it is imperative to promptly report the issue to the Incident Response Team. The Incident Response Team comprising of Team Leader/ Wing Chief (Strategic Planning), and representatives from IT section.
- xiv. **Access Revocation Procedures**  
Access to BIGM systems and data must be aligned with personnel changes to ensure security. Access revocation procedures are as follows:

**a. Termination of Employment:**

In the event of an employee's termination, access to all systems and data will be promptly revoked. Human Resources will notify the IT department immediately to initiate the access revocation process.

**b. Role Changes:**

Access privileges will be adjusted based on employees' roles. If there are changes in responsibilities or positions, the IT department will work in coordination with relevant departments to ensure access aligns with the current job requirements.

**c. Contract Termination:**

For contracted third parties, access will be revoked upon the completion or termination of the contract. The contracting department will notify the IT department in advance to facilitate the timely removal of access.

## 5.2 Server Access Policy

**i. User Authentication:**

Access office IT resources and services using distinct user accounts and strong passwords provided by the IT department. The IT Service Desk manages password specifications, complexity, length, and expiration.

**ii. Access Control:**

Implement role-based access control for file-based resources in Active Directory domains. Track and secure service access using access-control techniques like TCP.

**iii. Security Best Practices:**

Adhere to the rule of least access necessary for tasks. Prefer non-privileged accounts over root accounts.

**iv. Secure Access Channels:**

Use secure channels (e.g., SSH) for privileged access.

**v. System Maintenance:**

Keep the server operating system updated. Avoid unnecessary software installations on servers.

**vi. Performance Monitoring:**

Monitor server performance regularly, adjusting resources as needed.

**vii. Physical Security Measures**

To enhance the overall security posture of BIGM's server infrastructure, the following physical security measures must be diligently implemented:

**a. Access Control:**

Server rooms and data centers must be physically secured with restricted access limited to authorized personnel only. Use electronic access controls, biometric authentication, or keycard systems to ensure that only authorized individuals can enter server rooms.

**b. Surveillance Systems:**

Install surveillance cameras in and around server rooms to monitor and record access. Regularly review surveillance footage to identify any unusual activities or potential security breaches.

**c. Environmental Controls:**

Implement environmental controls, such as temperature and humidity monitoring, to ensure optimal operating conditions for servers. Adequate fire suppression systems should be in place to mitigate the risk of fire damage.

**d. Equipment Placement:**

Arrange servers and network equipment in a secure and organized manner within server rooms to facilitate efficient monitoring and maintenance.

### viii. **Third-Party Security Assurance**

BIGM recognizes the importance of ensuring that third parties with access to server resources uphold the same rigorous security standards as internal personnel. To maintain a high level of security assurance, the following guidelines are established:

#### a. **Security Assessment:**

Prior to granting access, third parties must undergo a comprehensive security assessment to evaluate their adherence to security best practices. Assessments may include a review of security policies, incident response capabilities, and other relevant security controls.

#### b. **Contractual Obligations:**

All third-party agreements must include explicit clauses related to data security, confidentiality, and compliance with BIGM's security policies. Contracts should clearly outline the consequences of security breaches and the responsibilities of third parties in maintaining the confidentiality of BIGM's information.

#### c. **Periodic Audits:**

Conduct periodic audits of third-party security practices to ensure ongoing compliance with established security standards. Work collaboratively with third parties to address any identified vulnerabilities or areas for improvement.

#### d. **Access Control for Third Parties:**

Grant access to third parties on a need-to-know basis, ensuring that access is limited to the resources required for their specific tasks. By adhering to these guidelines, BIGM aims to establish a robust security framework that encompasses both internal and external entities accessing server resources.

## 5.3 Network Access Policy

To safeguard BIGM's network infrastructure, the following access policies and security practices are implemented:

### i. **Least-Privilege and Access Controls:**

Adhere to the least-privilege concept and implement access control procedures for network access. Configure access controls to allow only authorized individuals to access and modify data based on its sensitivity.

### ii. **Authentication via VPN:**

Authenticate employees and contracted third parties using VPN for secure remote access to office networks.

### iii. **Network Segregation:**

Implement network segregation based on security research recommendations to isolate and protect critical segments of the network.

#### a. **Network Routing Controls:**

Utilize network routing controls to support access control policies, ensuring efficient and secure data transmission.

#### b. **Remote Administration:**

Perform remote administration over secure channels, employing encrypted network connections such as SSH for enhanced security.

#### c. **DMZ Setup:**

Establish a Demilitarized Zone (DMZ) using a high-performance firewall to enhance network security, segregating external and internal network traffic.

**d. Logging and Audit Trails:**

Log security-related events and maintain audit trails in InfoSec-approved logs for monitoring and investigation purposes.

**e. Patch Management:**

Install patches or hotfixes as advised by InfoSec and equipment manufacturers to address vulnerabilities and enhance network resilience.

**iv. Regular Security Audits and Assessments**

To continually assess and improve the security posture of BIGM's network, the following practices are established:

**a. Audit Scope:**

Define the scope of security audits, covering network infrastructure, access controls, and data handling practices, and policy compliance.

**b. Frequency:**

Conduct periodic security audits based on the risk profile of BIGM's operations and evolving threat landscape.

**c. Independent Assessment:**

Engage external security experts or auditors to provide an unbiased evaluation of network security, aligning with least-privilege concepts and access control procedures.

**d. Vulnerability Scanning:**

Utilize vulnerability scanning tools to identify and remediate potential weaknesses in the network infrastructure.

**e. Incident Response Testing:**

Include incident response testing in security assessments to evaluate the effectiveness of response procedures during simulated security incidents.

**f. Documentation and Reporting:**

Maintain comprehensive documentation of audit findings, remediation actions, and implemented improvements. Generate regular reports for senior management and stakeholders to ensure transparency on the network's security status.

**g. Continuous Improvement:**

Use audit findings to drive continuous improvement initiatives, enhancing security controls and addressing emerging threats.

#### 5.4 Enterprise Resource Planning (ERP) Access Policy

The ERP Access Policy outlines the secure utilization and management of BIGM's ERP software. This policy aims to ensure the confidentiality, integrity, and availability of sensitive information.

**i. ERP Software Utilization:**

Utilize the designated BIGM server to run ERP software, ensuring a centralized and secure environment for data processing.

**ii. Remote Access via Web-based Applications:**

Employ web-based ERP applications for remote access, allowing authorized personnel to securely access the system from different locations.

**iii. Real-time Data Reporting:**

Leverage the ERP system for generating real-time data reports on various aspects, including student management, faculty, inventory, HR, payroll, and finance.

**iv. Data Integrity Preservation:**

- Implement techniques to ensure the integrity of data stored within the ERP system, safeguarding against unauthorized alterations.
- v. **Detection of Unauthorized Access:**  
Establish mechanisms for detecting and preventing unauthorized access and exploitation of sensitive ERP data, ensuring robust security measures.
  - vi. **Strong Passwords and Role-based Authorization:**  
Maintain the security of the ERP system by enforcing strong password policies and role-based authorization to control access privileges.
  - vii. **Staff Training for Internal Breach Risks:**  
Conduct regular training sessions for staff to enhance awareness and reduce internal breach risks, fostering a security-conscious culture.
  - viii. **Standardized Data Reporting Formats:**  
Standardize data reporting formats within the ERP system to ensure consistency and facilitate efficient data analysis.
  - ix. **Data Cleansing and Continuous Maintenance:**  
Implement data cleansing and continuous maintenance strategies to enhance data quality and reliability over time.
  - x. **System Operations and Maintenance:**  
Consider system operations and maintenance activities that contribute to data quality, reliability, and the overall performance of the ERP system.
  - xi. **Verification and Validation of Data Inputs:**  
Institute procedures to verify and validate data inputs to guarantee accuracy and reliability of information processed by the ERP system.
  - xii. **Regular Audit Trail Testing:**  
Test audit trail functionality regularly to ensure its effectiveness in capturing relevant system activities for security and compliance purposes.
  - xiii. **Use Encryption for Data Integrity**  
Employ robust encryption protocols to maintain data integrity across the organization, ensuring the secure transmission and storage of sensitive information.
  - xiv. **Secure Disposal of Data and Equipment**  
Ensuring the secure disposal of data and equipment is paramount to maintaining the confidentiality and integrity of information. The following guidelines are established:
    - a. **Data Disposal Procedures:**  
Define clear procedures for the secure disposal of sensitive data stored within the ERP system. Implement secure deletion methods or utilize data shredding techniques to irreversibly remove data from storage media.
    - b. **Physical Media Destruction:**  
Mandate the secure destruction of physical storage media (e.g., hard drives, tapes) containing ERP data to prevent data recovery.
    - c. **Documentation and Verification:**  
Maintain detailed documentation of the disposal process, including records of data erasure or physical destruction. Conduct periodic audits to verify and ensure compliance with secure disposal procedures.
    - d. **Equipment Decommissioning:**  
Establish a process for decommissioning ERP-related hardware or equipment, ensuring proper disposal or repurposing in alignment with security protocols.

**e. Employee Training:**

Provide training to employees involved in the disposal process, emphasizing the importance of securely handling and disposing of ERP-related data and equipment.

**xv. Secure Communication Guidelines**

To safeguard communication within the ERP system, the following secure communication guidelines are implemented:

**a. Encryption Protocols:**

Utilize strong encryption protocols for data transmitted within the ERP system to prevent unauthorized access or interception.

**b. Secure Channels:**

Implement secure communication channels, such as Virtual Private Networks (VPNs) or encrypted connections, to protect data in transit.

**c. User Authentication:**

Enforce robust user authentication mechanisms to ensure that only authorized personnel can access and communicate within the ERP system.

**d. Access Controls:**

Implement access controls within the ERP system to restrict communication privileges based on user roles and responsibilities.

**e. Audit Trails:**

Maintain comprehensive audit trails of communication activities within the ERP system for monitoring, detection, and investigation purposes.

**f. Regular Security Audits:**

Conduct regular security audits to assess the effectiveness of communication security measures and identify areas for improvement.

**g. Employee Awareness:**

Raise employee awareness about secure communication practices within the ERP system through training programs and communication campaigns.

**h. Incident Response Procedures:**

Establish clear incident response procedures for addressing and mitigating security incidents related to communication within the ERP system.

## 5.5 Application Access Policy

**i. Web Application Availability:**

Ensure that necessary web applications for job tasks are accessible to all office personnel and contracted third parties.

**ii. Access to Sensitive Panels and Systems:**

Grant access to sensitive web admin panels and systems for office personnel and contracted third parties only with senior management's consent and if deemed necessary for their roles.

**iii. Segregation of Sensitive Systems:**

Physically or logically segregate sensitive systems to limit access exclusively to authorized individuals.

**iv. Regular Updates for Web Applications:**

Implement a continuous update process for web applications to keep them current with events or programs.

**v. Optimized Web Application Speed:**



- Prioritize the optimization of web application speed, recognizing that user experience begins with swift application responsiveness.
- vi. **Management of Web Application Issues:**  
Highlight current issues in the web application, preventing deletion of old issues and mandating their retention in an inactive state.
  - vii. **Regular Backups for Web Applications and Databases:**  
Conduct regular backups for both web applications and databases to ensure data recovery in the event of disruptions or data loss.
  - viii. **SSL Implementation:**  
Enforce the use of Secure Sockets Layer (SSL) for web applications to enhance the security of data transmission.
  - ix. **Validation Policy for Data Integrity:**  
Implement a validation policy within the web application to prevent the entry of bad data into the database, ensuring data integrity.
  - x. **File Size Restrictions:**  
Define specific size limitations for document or file uploads to the web application, preventing the uploading of excessively large files.
  - xi. **Remote Work Security Practices**
    - a. **Secure Remote Access:**  
Utilize Virtual Private Network (VPN) connections for secure and encrypted communication when accessing BIGM's network remotely.
    - b. **Multi-Factor Authentication (MFA):**  
Make Multi-Factor Authentication (MFA) mandatory for remote access to enhance user authentication.
    - c. **Endpoint Security:**  
Ensure that devices used for remote work have updated antivirus software and security patches. Encourage the use of company-approved endpoint protection tools to guard against malware and cyber security threats.
    - d. **Data Encryption:**  
Implement encryption measures for sensitive data during transmission and storage on remote devices. Emphasize the use of encrypted communication channels and protocols to protect data integrity.
    - e. **Remote Collaboration Security:**  
Utilize secure collaboration tools with end-to-end encryption for virtual meetings and document sharing. Educate employees on the secure use of communication platforms and sharing sensitive information during remote collaboration.

## 5.6 Other Policies

### i. Printers Access Policy

Collect printed paper promptly to prevent security issues. b. Service printers periodically.

### ii. Wi-Fi Access Policy

a. Restrict mobile Wi-Fi access, providing access only to specific individuals through the IT department.

- b. Monitor and control Wi-Fi usage to prevent unauthorized access and maintain a secure network environment.
- c. Implement mechanisms to detect non-official work on mobile devices accessing the network.
- d. Promptly stop Wi-Fi access if non-official work is detected to mitigate potential security risks.
- e. Allow Wi-Fi permission for only one mobile device per user to regulate and monitor network access.
- f. Enforce strict controls on the number and type of devices authorized for Wi-Fi connectivity.

## 6. Reporting Requirements

To ensure robust incident management and a continuous enhancement of our data security measures, BIGM has established the following reporting procedures. The incident response team and IT department play pivotal roles in creating and managing reports at various intervals.

### i. Daily Incident Reports

#### a. Responsibility:

Incident response teams or the IT department at BIGM are tasked with the creation and management of daily incident reports.

#### b. Action:

Promptly document and assess daily incidents to facilitate a swift response and resolution.

### ii. Weekly Incident Reports to Director

#### a. Compilation:

Compile and send comprehensive weekly incident reports to the director of BIGM

#### b. Content:

Provide a consolidated overview of the week's incidents, highlighting trends and areas of concern.

### iii. High-Priority Incident Alert

#### a. Immediate Action:

Immediately alert the IT officer at BIGM for high-priority incidents that demand urgent attention.

#### b. Objective:

Ensure a rapid response to critical incidents to minimize potential impact.

### iv. Monthly IT Security Report

#### a. Generation:

Generate a monthly report at BIGM detailing the number of IT security issues encountered and the resolutions implemented.

#### b. Insights:

Provide insights into the overall state of IT security, fostering a proactive approach to addressing recurring issues.



**v. Regular Policy Review and Updates**

**a. Communication:**

Clearly communicate at BIGM that the data security policy undergoes regular reviews and updates.

**b. Engagement:**

Encourage active participation and feedback from users and stakeholders at BIGM to enhance the policy's effectiveness over time.

**c. Emphasis:**

Emphasize at BIGM the collaborative nature of policy reviews to adapt to evolving threats and industry best practices.

By adhering to these reporting procedures and cultivating a culture of continuous improvement, BIGM aims to fortify its incident response capabilities and uphold the highest standards of data security.

### Definitions of Terms

**Data** — Data is a collection of a distinct small unit of information. In general, data is any set of characters that is gathered and translated for some purpose, usually analysis. In a computer's storage, digital data is a sequence of bits (binary digits) with a value of one or zero. Data is processed by the CPU, which uses logical operations to produce new data (output) from source data (input).

There are multiple types of data. Some more common types of data include the following:

- Single character
- Boolean (true or false)
- Text (string)
- Number (integer or floating-point)
- Picture
- Sound
- Video

**Data Security** — Data security is the process of protecting official important data and preventing data loss through unauthorized access. This includes protecting data from attacks that can encrypt or destroy data, such as ransomware, as well as attacks that can modify or corrupt data. Data security also ensures data is available to anyone and access to it.

**ACL** — ACLs were the only way to achieve firewall protection. Today, there are many types of firewalls and alternatives to ACLs. ACL in conjunction with technologies like VPN that specifies which traffic should be encrypted and transferred through a VPN. ACL identifies a trustee and specifies the access rights allowed, denied or audited for that trustee.

**Database** — A database is an organized collection of data so that it can be easily accessed and managed. Data can be organized into tables, rows, columns, and indexed to make it easier to find relevant information. The main purpose of the database is to operate a large amount of information by storing, retrieving, and managing data.

**Encryption**—The process of encoding a message or other information so that only authorized parties can access it.

**Firewall** — A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between the internal network and incoming traffic from external sources in order to block malicious traffic like viruses and hackers.

**Network segregation** — The separation of the network into logical or functional units called zones. For example, there might be a zone for sales, a zone for technical support and another zone for research, each of which has different technical needs.

- **RBAC** — Role-Based Access Control restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that employees have to the network.

- **Server** — A server is a software or hardware device that accepts and responds to requests made over a network. The device that makes the request and receives a response from the server is called a client. On the Internet, the term server commonly refers to the computer system that receives requests for a web file and sends those files to the client.
- **VPN** — VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPN encrypt internet traffic and disguise online identity. This makes it more difficult for third parties to track activities online and steal data.
- **VLAN (Virtual LAN)** — VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.
- **ERP** - Enterprise Resource Planning refers to a type of software that BIGM use to manage day-to-day activities such as Accounting, Human Resource Management, Payroll, Student Management, Faculty Management, Library and Inventory. A complete ERP suite also includes enterprise performance management, software that helps plan, budget, predict, and report on an organization's financial data, student admission data, employee attendance and so on.
- **DMZ** - A DMZ or demilitarized zone is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic.
- **CPU** - CPU is short for Central Processing Unit. It is also known as a processor or microprocessor. It's one of the most important pieces of hardware in any computing system – if not the most important.
- **Ransomware** - Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
- **Wi-Fi** - is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearable), and other equipment (printers and video cameras) to interface with the Internet.
- **TCP** - Transmission Control Protocol is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.
- **SSH** - The Secure Shell protocol is a network protocol that provides a secure interface between users and computers on unsecured networks, particularly for system administrators. The SSH protocol is also implemented by a set of utilities. A Secure Shell connection can be encrypted between two computers connected over an open network, like the internet, with strong password authentication and public key authentication. Besides providing strong encryption, SSH is also widely used to manage systems and applications remotely, enabling

network administrators to access another computer via a network and execute commands, as well as move files.

- **LAN** - A local area network (LAN) consists of a series of computers linked together to form a network in a circumscribed location. The computers in a LAN connect to each other via TCP/IP Ethernet or Wi-Fi.

  
Dr. Krishna Gayen  
Sr. Research Fellow  
Bangladesh Institute of  
Governance & Management

  
Dr. Mohammad Tareque  
Director  
Bangladesh Institute of  
Governance and Management (BIGM)

C



---

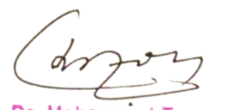
**Bangladesh Institute of Governance and Management (BIGM)**

E-33, Syed Mahbub Morshed Sharoni, Agargaon, Sher-E-Bangla Nagar, Dhaka-1207

PABX: 880-2-223374041-44 (Ext:102, 106, 107, 114), Email: [info@bigm.edu.bd](mailto:info@bigm.edu.bd)

[www.bigm.edu.bd](http://www.bigm.edu.bd)

  
Dr. Krishna Gayen  
Sr. Research Fellow  
Bangladesh Institute of  
Governance & Management

  
Dr. Mohammad Tareque  
Director  
Bangladesh Institute of  
Governance and Management (BIGM)

D