Objectives of cyber security

A cybersecurity plan is critical and valuable for any company with highly sensitive information. Many companies created a post for chief security officer (CSO) or chief information security officer (CISO) to ensure their cybersecurity.

Cyber security is becoming strategic field for Bangladesh, especially, with the recent increasing interest in e-commerce and e-government. We find the best way to explain some complex concepts is to use an adequacy. So, people can quickly relate to some embodied things in our daily life and get the core ideas. Now, let me try to explain strategy, program, and project as follows:

In today's increasingly virtual world, a Cyber Security Specialist's job is vital to the web-safety of everyone everywhere. As a Cyber Security Specialist, we are responsible for secure businesses' computer dealings by increasing a secure system and building up to date with all of the latest technology and innovation out there. Potential employers are looking for someone who can provide the right talents to their company and showing these in a well-written resume objective is the best method to be done it.IT network architecture and in-network and service security, to provide support to the cyber security team.

Almost immediately after cyber security technology is introduced, its usage is declared industry standard by some regulatory body, and this locks organizations into the identified countermeasure approach.

Hopeful for a Cyber Security Specialist position at Boeing; coming with 1year internship experience, great communication skills, and proficiency in all Microsoft Office tools, as well as high attention to detail. it might be expected that policymakers are constantly confronted with decisions on how to react to the latest threat. However, because it is often the case that decisions concerning cyber security measures are delegated to technologists, a policymaker may not actually see these decisions being made, and thus not have a chance to weigh in on the organizational impact of various alternative approaches

Security & Privacy Plan

Hackers are sent anonymously to the front server in the corporate network without being authenticated or inspected. Once allowed, these requests, which might contain malicious code, can pass through DMZ firewalls with no control.

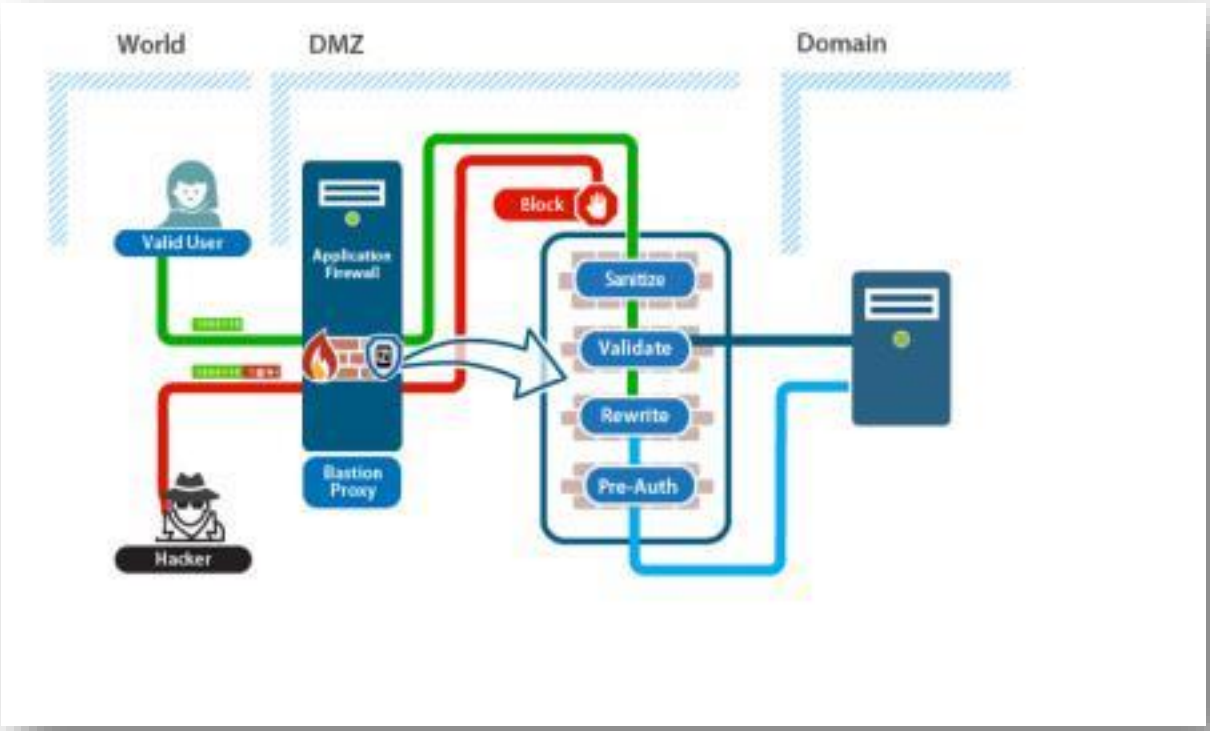


Fig: Application Firewall

The application firewall will have the following security layers:
Request rewrite – session termination in the DMZ and rewrite of the request that is sent to the domain

- Protocol level sanitization – inspecting the traffic to validate the structure of the traffic as expected by the protocol
- Application level inspection – validating that the data content matches what is expected by the server
- Device pre-authentication – performing device validation before allowing any request to enter the domain

In order to ensure that no malicious code is injected into a request, the solution passes each request through multiple security inspections and validation channels, including session termination and rewrite, protocol sanitation, data validating and device pre-authentication. By doing so, the risk of most protocol and application level attacks is eliminated.

Also, below Security will be ensured:

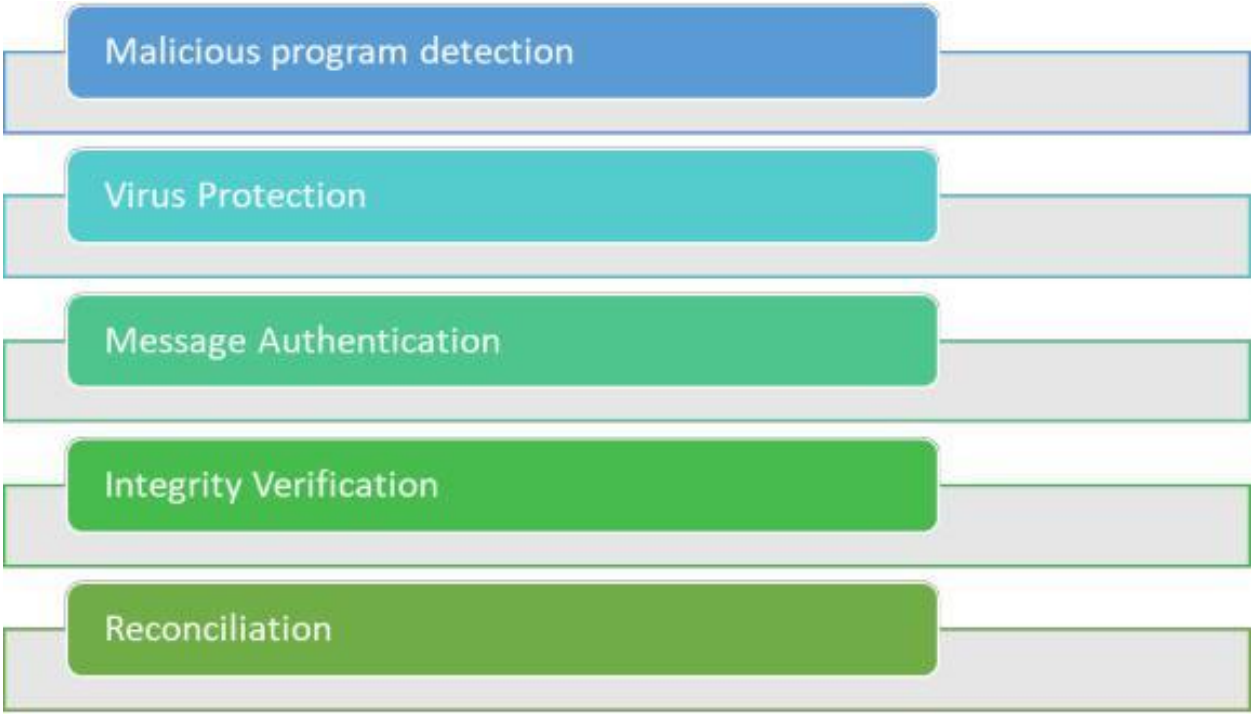


Fig: Security Plan

Integration Plan

Information exchange will be a model of collaboration between BUSINESS AUTOMATION and their stakeholder that will minimize the need for the permit applicant to serve as documents and information delivery media. The information exchange will be the procedures of accessing information directly from the BUSINESS AUTOMATION portal which will serve as electronically by integrating with electronic registries and information systems.

For implementing BUSINESS AUTOMATION Online Customer Service Management, it is necessary to establish electronic data exchange with the following state institutions:

- **Existing System:** to establish data exchange of land calculation, online application, bill of material collection, auto generate e-bill, bill payment, mobile app of BUSINESS AUTOMATION and Other Concern Stakeholders.

The stakeholder will provide Application Programming Interfaces (APIs) for connecting other electronic registries and systems to be able to exchange data if such a need will appear in the future.

Besides the data exchange with the external information systems, the BUSINESS AUTOMATION eService will be integrated with the existing horizontal/shared electronic services such as Payment Gateway and PKI services. The BUSINESS AUTOMATION eService will be implemented to allow developing any needed interfaces to exchange data with external information systems in the future.

User Interface (UI) & User Experience (UX) Plan

After finishing requirement collection we will develop a UI & UX for **BUSINESS AUTOMATION Online Customer Service Management**. As we are planning Agile methodology in our proposed development so, after each module requirement collection we will develop User Interface & User Experience iteratively.

After completing requirement collection of each phase, our System Analyst, Business Analyst and UI expert & UX expert will analysis the requirement to prepare a user-friendly User Interface & User Experience.

- ✓ Once the project's concept is clear we move to the brainstorming area, to transform our ideas regarding your interface into reality. We bring a pen and a piece of paper. That's more efficient in terms of time compared to the advanced tools such as Balsamiq Mockups, Sketch, Photoshop etc.

Fig: UI & UX work flow

- ✓ We will also validate the sketch between URS flow design and also with BUSINESS AUTOMATION authority

- ✓ When customer confirms the structure and the flow—that's a signal to move forward. Then we will design the interface.

- ✓ At this stage we make a presentation of our versions of the design.

Then we will mockup the design for creating the prototype of the system and will validate by BUSINESS AUTOMATION authority.

Hosting Architecture & Plan

A detail hosting plan for the BUSINESS AUTOMATION Online Customer Service Management system is given below

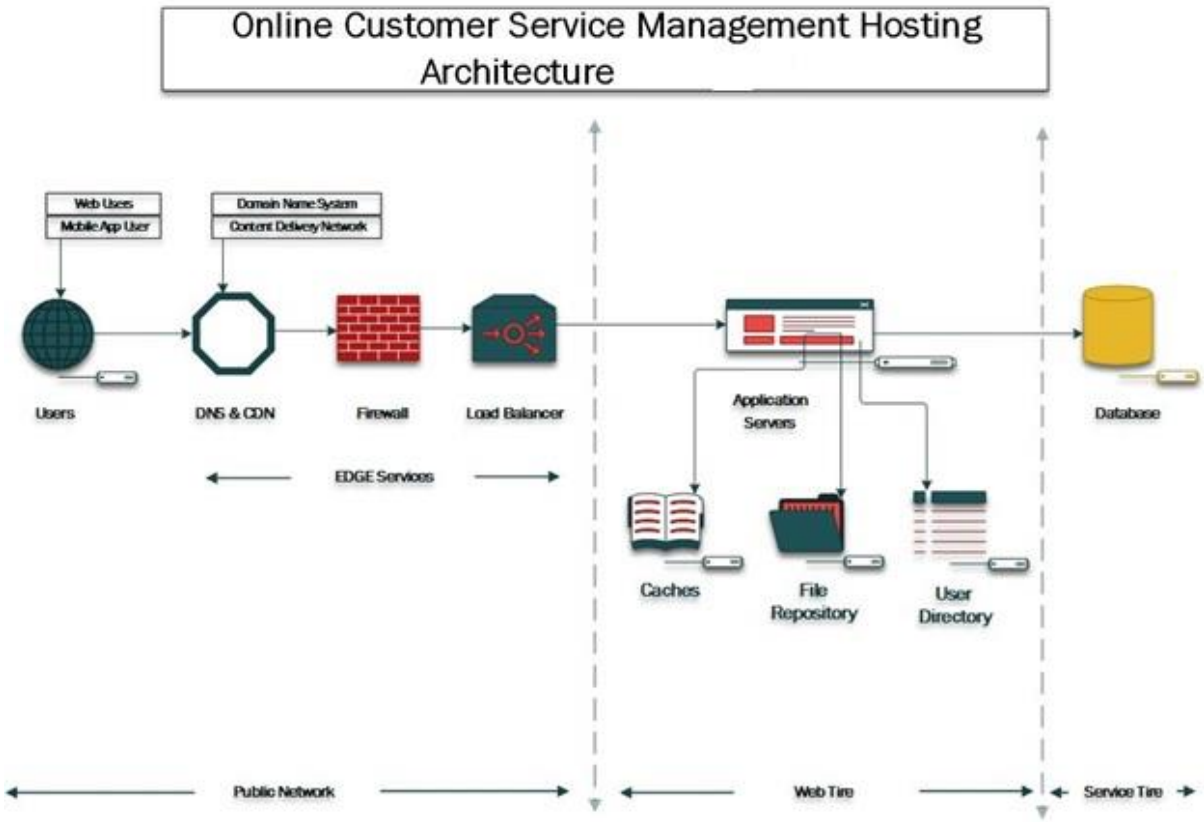


Fig: Web Hosting Architecture Plan (Software)

- User sends a request to a specified URL.

- Edge Services receives the request – Edge services consist of a group of services that handle the request and get it to the right destination.
- These include: the domain name server, the CDN server, the firewall, and the load balancers. Every request going to or from the network goes through the firewall.
- Domain Name Server (DNS) –The domain portion of the URL is resolved into an IP address via the Domain Name Service (DNS). This IP address may actually be the IP address of a CDN server, load-balancer, firewall, or proxy service in-front of the actual web application server that will satisfy the request.

- Firewall – The firewall evaluates the packets that form the request and allows only those packets which meet the rules of the firewall to continue forward to the load balancer. Typical rules might only pass incoming HTTP and HTTPS packets destined for ports 80 and 443. Firewalls often have two sets of rules, one for filtering inbound traffic into the firewall and one for filtering outbound traffic going from the firewall. Generally, DNS resolution for internal requests is typically done using a private DNS server rather than a public DNS server.

- Security - Security is enabled across multiple layers through a defense in depth approach. Applications have their access provided to the right users and roles through identity and access management. The web applications are protected from threats (such as cross site scripting, SQL injection attacks, and more) starting at the beginning of the development cycle. The application stack is further isolated at the network level into multiple network segments or VLANs. The sensitive data is protected from end users and privileged users. Continuous monitoring of threats and log analysis in the solution provide visibility and actionable intelligence. Logs are used for audit and compliance reports

- Load Balancers – The load balancer sends the request to a specific web application server in a pool of web application servers. The decision is made using a random or 'round robin' algorithm, or some other method.

- Web Application Servers – The web application server returns a resource (normally some form of web content) based on the user's request. Based on the request, the web server retrieves the static content by accessing the file system or invokes a program or service to generate dynamic requested content.

- Before any processing is done, the web application server may invoke the user directory to authenticate the user and validate permission rights to perform the request. Typically, this is done as a part of a login process, which establishes a session used for a series of requests. The user directory may use security services and the enterprise user directory in the enterprise.

- The web application server determines if the request can be satisfied by a local cache. If so, the appropriate content and associated data is returned to the user.
- File repositories, like caches, store and managed data that can be requested by the application server. Caches and file repositories return data through the firewall. If application logic must be invoked (by the application server) then retrieval of data from files, databases, web-services, sensors, and other sources of data as well as programmatic generation of new data or information may be required.

- Transformation and Connectivity takes the messages and data intended to be stored in the database and completes any necessary transformation from web formats to data base formats and ensures secure reliable messaging is used appropriately.

- Data – The web application server may need to access a database to query data in order to generate the requested response. That data may be accessed directly or may require transformation in order to be utilized by the application. Data includes logs and data bases to enable analytics.

- **Data-growth and Scalability Plan:**
    - Right server up front: Scalable specification needed at the time of implementation of servers.

- Storage Facilities: Redundant and Scalable Storage Array with stable RAID facilities and redundant controller units for Network based block storage and other types of storage. Scalability for extending Disk or Disk Spaces.

- Network and Bandwidth: Scalable Network infrastructure facility with sufficient bandwidth for future growth.

- **User Handling/ Load Balancing Mechanism:**
    - We suggest to use Barracuda Load balancing Mechanism which is Highly demanding enterprise networks full-featured application delivery controller that optimizes application load balancing and performance while providing protection from an ever-expanding list of intrusions and attacks.

    - The Barracuda Load Balancer ADC is a Secure Application Delivery Controller that enables Application Availability, Acceleration and Control, while providing Application Security Capabilities.

    - Barracuda Load Balancer is available in hardware, virtual and cloud instances, it provides advanced Layer 4 and Layer 7 load balancing with SSL Offloading and Application Acceleration. The Application Security module ensures comprehensive web application protection, including against OWASP Top 10 and Application DDoS attacks, while monitoring outbound traffic for Data Loss Prevention.

- **Licensing issues:**
    - The bellow mentioned appliances and systems need license:
    - Operating Systems License.
    - Virtualization Appliances License. (If needed)
    - Firewall License.
    - Router License.
    - Load Balancer License.
    - Database Enterprise Licensing.
    - Network Monitoring Software License.

- **Schedule Backup and restore Requirements:**

Our recommended Backup Plans are:

  - Perform full backups of all data on a weekly basis. The fourth full backup per month becomes a monthly backup.
  - Perform incremental backups on a daily basis - an incremental backup is defined as the backup of all data changed since the last backup.
  - If possible, stagger the weekly full backups throughout the week to balance resource utilization.

- **Backup Retention periods are:**
  - Retention period for daily incremental backups - one month
  - Retention period for weekly full backups - three months
  - Retention period for monthly full backups - one year

- **Backup Requirements:**
  - For Physical Server Failure a replica of all VMs should be placed on single or more Physical Servers.
  - For Storage Failure storage array must have redundant disks and/or controllers to protect against single points of failure within the array.
  - A Replication of DATA or Databases should be stored on different place if full storage array meet with a massive failure.

- **Restore requirements:**
  - A restore will performed to return data that will have been lost, stolen or damaged to its original condition or to move data to a new location.
  - It's necessary to test the restore process and the data recovery tools regular manner.
  - Protection copies should be randomly checked at various points in time to ensure they meet recovery point objectives.
  - All applications must be checked before doing an actual data restore to ensure they will be able to use the restored data.

- **Circumstances that lead to the need for a data restore:**
  - Human error, where data is accidentally deleted or damaged.
  - Malicious attacks where data is exposed, stolen or infected.
  - Poour outages
  - Manmade or natural disasters
  - Equipment theft, malfunctions or failures

- Firmware corruption

- **Disaster Recovery Requirement:**
  - Required a back-up data center (hot site) to be used in the event such a disaster does occur.
  - Physical Security - includes access control, fire prevention and protection, electrical failure protection, etc.
  - Emergency Procedures - documentation and training pertaining to handling emergency situations.
  - Problem Diagnosis - procedures for determining the cause, forecasting the extent, and proceeding with remedial actions for any hardware, or software outage.
  - Off-site Storage System - maintaining, documenting, and supporting facilities for providing storage and retrieval of data off-site from the central data center.
  - Recovery Centre - providing the facilities for back-up of the central data center.
  - Documentation - set of procedures pertaining to the ability to provide contingency recovery at the back-up data center.
  - Available manpoour - in a disaster situation, how additional manpoour will be obtained and used.
  - Testing - periodic testing of the various aspects of the Disaster Recovery Plan.

- **Monitoring tools requirements:**
  - For monitoring purpose here's a list of the Top IT Infrastructure Monitoring Tools & Software
  - Solarwinds Network Performance Monitor
  - Solarwinds Server and Application Monitor
  - WhatsUp Gold
  - Nagios XI
  - Zabbix

- Bellow minimum features are required:
  - Host add delete by snmp v2.
  - Host Interface Bandwidth utilization graph with Network Analyzer for Nagios.
  - Scheduled Reporting.
  - Host alert up/down and critical alert notification over the mail.
  - Topology MAP view all connected host with up and down state.
  - Host health check and interface status view.
  - Basic administration and operational base knowledge sharing session.

Web Hosting Architecture Plan (Hardware)

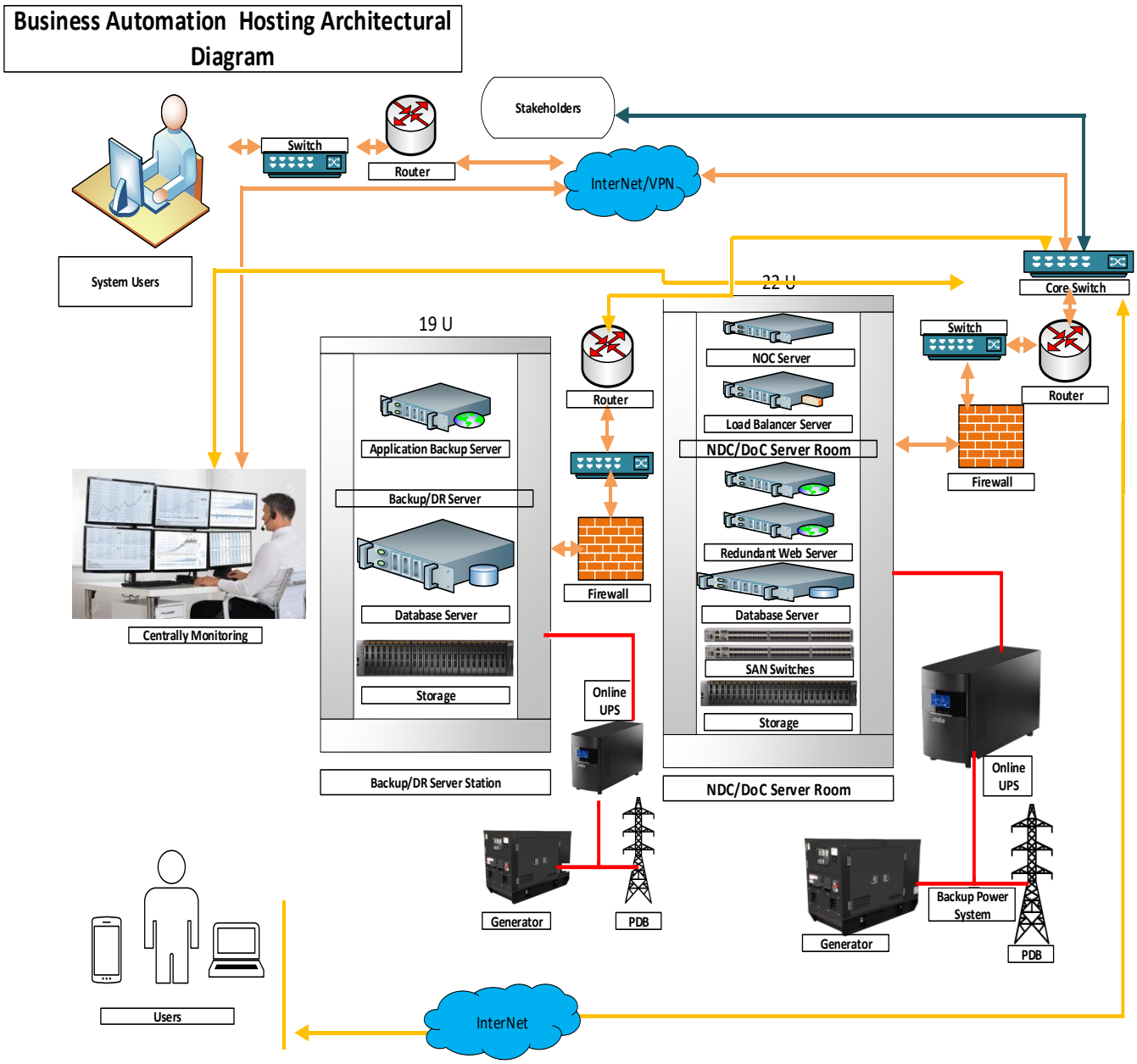


Fig: Web Hosting Architecture Plan (Hardware)

Load Balancing with HAProxy for High-Availability

- HAProxy is well-known for its stability, reliability and performance in terms of CPU and memory usage.
- It is widely used by high-traffic websites such as Tumblr, Twitter, Stack Overflow, GitHub
- HAProxy supports client-side SSL encryption as server side.
- It manages many extensions to TLS, such as NIS, NPN / ALPN and OCSP, including the validation of server-side certificates and client-side certificates.

- It is possible to use either IPv4 or IPv6 or the socket UNIX client side as server side
- Provides a comprehensive list of 61 different metrics
- The status page is much more detailed and user-friendly
- Easily able to integrate with third-party monitoring services like Datadog

Servers for Web Hosting and Database

- For single server installations at least two Intel Xeon 64-bit CPU, 12 Core, 2.4GHz, 32MB L3 Cache Memory
- RAM requirements: For single server installations, a minimum of 32 GB * 8 = 256GB
- At least 1 TB free disk space for each server configured with RAID-5
- Dual Redundant Poour Supply.
- 16 GBps Fiber Channel host bus adapters dual port.
- SAS HBAs and RAID adapters supported.
- Integrated virtualization or Virtualization supported.
- Integrated Management Module for advanced service-processor control, monitoring, and alerting functions as well as remote controlling.
- PCI Expansion slots availability
- Standard Integrated Colling System.
- 4 x 10GbE Network Adapter.
- Hot-swap parts - Drives, poour supplies, and fans.

Storage System

- RAID 0, 1, 5, 6 and 10: Supports Distributed RAID 5 and 6
- Minimum 8TB storage space configured with RAID 5
- Minimum 32GB Cache Memory.
- Dual-port, hot-swappable, 12 Gb SAS disk drives
- SAN-attached 8 or 16Gbps Fiber Channel, 1 Gbps iSCSI and optional 10 Gbps iSCSI/FCoE
- Web-based graphical user interface (GUI)
- Dual controller.
- Fully redundant, hot-swappable Poour supply and Cooling System.
- Supported intermix of SAS disk drives.

SAN Switches:

- high-performance, flexible, highest port density and lowest poour consumptions compact SAN Switch.

- Nonblocking architecture, with all 1/2/4/8/16-Gbps ports operating at line rate concurrently.
- intelligent storage networking capabilities such as virtual SANs (VSANs), Inter-VSAN Routing (IVR), link aggregation using Port Channels, quality of service (QoS), and security.
- Smart Zoning
- Nondisruptive software upgrades, dual redundant hot-swappable poour supplies (with integrated fans), dual redundant hot-swappable fan trays, VSANs for fault isolation, Inter-VSAN Routing (IVR) for sharing resources across VSANs, Port Channels for Inter-Switch Link (ISL) resiliency, and F-port trunking for resiliency on uplinks.
- Industry-leading intelligent diagnostics such as Fiber Channel ping, Fiber Channel traceroute, Switched Port Analyzer (SPAN), Cisco Fabric Analyzer, and an integrated Call Home capability to enhance reliability, facilitate faster problem resolution, and reduce service costs.

Firewall

- Minimum Firewall Throughput (Packet per Second) 82.5 Mpps
- Minimum Firewall Throughput 80 / 80 / 55 Gbps
- Minimum Concurrent Sessions (TCP)12 Million
- Minimum New Sessions/Second (TCP) 300,000
- Minimum SSL-VPN Throughput 4 Gbps
- Antispam
- Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, Virus Outbreak Protection
- Web Filtering
- IPS Service
- App Control Service

Router

- Services integration with voice, video, security, mobility, and data services.
- High-performance multicore processors for high-speed WAN connections.
- Embedded IP Security (IPsec) VPN hardware acceleration.
- Minimum 4 GB DRAM and 4GB Flash Memory
- Network Interface Modules (NIMs) for flexible configurations.
- At least four built-in 10/100/1000 Mbps RJ-45 ports; 2 x 1G optical ports with SFP, Ethernet ports for WAN or LAN.
- Enhanced High Speed WAN Interface Card

Network Switch manageable

- Must have minimum 24 10/100/1000 Mbps RJ-45 ports
- Maintain International Quality Environmental Safety standard
- Must have Redundancy Poour Supply Units (PSUs), field-replaceable poour supplies
- Must support Standard SFPs like including QSFP, SFP+, 1000BASE-T SFP, Gigabit Ethernet SFP
- Switching capacity (data rate, full duplex) Min. 200 Gbps
- Forwarding capacity (data rate, full duplex) Min. 60 Mbps (wire speed)

Application Compliance Requirements

Web Application

- We will provide a web-based solution which will be hoisted in a centralized web-server.
- The application will support MVC framework.
- The application will be developed following Service Oriented Architecture. (SOA)
- Considering the operating/client environment at different level of this application, we will develop the application in such a way so that it requires low bandwidth to run
- The web-based application will support cross browser platforms (web-browsers such Mozilla Firefox, Opera, Chrome, internet Explorer, Safari etc.)
- The application will have ability to seamless integration with future module / components / applications the application will be lightweight and rich client-side scripting
- UI will be developed based on the analysis of UX.
- All web interface of this application will be fully responsive

Sizing, Performance and Scalability Requirements

- Our system will be capable of handling online functionalities for a database of at least 100,000/year service recipients and in terms of service provide 64 Offices and 592 System Users.
- Our system processing shall be scalable to support the volume estimates for a period of 10 years at a 20% annual growth rate.
- We will design to handle estimated 10,000 simultaneous connection when it is ultimately rolled out.
- We will conduct an extensive load testing task taking above factors into consideration and submit a load testing result
- The database architecture will be such that the system will available to user 24x7x355 days a year without any unapproved downtime

- Page load time, login response-time, on-click load time for the web application will be less than 5 seconds while this is accessed over the intranet.
- Average transaction response time, on-submit response-time, or any other database access/ search time will be less than 7 seconds when the system solution is accessed over the intranet.
- Considering the network infrastructure challenges in Bangladesh, the solution will support low bandwidth conditions for the services defined in the functional requirements.
- In case of mobile application also, this will also support very low bandwidth even in 2G network provided internet bandwidth.
- The solution will have highly scalable to accommodate current and future requirements within the scope of the scope mentioned in TOR
- We have analyzed the requirements whether both horizontal scaling (Scan Up) and vertical scaling (Scan Up) which will be required for this e service application.
- The e-Service application will provide with appropriate caching mechanism to handle very high-traffic scalability

Network -Security Policy

Version 1

Owner: Information and Security Team

Business Automation Ltd.

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
I	December 2018	Md. Shiful Islam	New Policy

Review Distribution

Name	Title
Md. Shiful Islam	Head of Information and Security
Md. Mithu Pramanik	Head of Implementation and Support

Approval

Name	Position	Signature	Date
Mr. Jahidul Hasan	CEO		

Document name:	**Network Security Policy**
Document type:	**Policy**
Staff group to whom it applies:	**All staff within the Organization and Its managed Organization**
Distribution:	**The whole of the Organization**
How to access:	**Intranet**
Issue date:	**December 2018**
Next review:	**March 2019**
Approved by:	**Executive Management Team**
Developed by:	**Information and Security Team – Business Automation Ltd.**
Director leads:	**Chief Executive Officer**
Contact for advice:	**Information and Security Team – Business Automation Ltd.**

NETWORK SECURITY POLICY

1 Introduction

1.1 This document defines the Network Security Policy for Business Automation Ltd.'s (referred to hereafter as the BAT). The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support and are Users of the network.

1.2 This document:

a. Sets out the Organization's policy for the protection of the confidentiality, integrity and availability of the network;
b. Establishes the security responsibilities for network security;
c. Provides reference to documentation relevant to this policy.

1.3 The network is a collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by cables or wireless devices. The network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

2 Purpose/Scope of this Policy

2.1 The purpose of this policy is to ensure the security of The BAT's and its managed Organization's network. To do this the BAT will:

a. Ensure Availability
   Ensure that the network is available for Users;
b. Preserve Integrity
   Protect the network from unauthorised or accidental modification;
c. Preserve Confidentiality
   Protect assets against unauthorised disclosure.

2.2 The purpose of this policy is also to ensure the proper use of the BAT's and its managed Organization's network and make Users aware of what the Organizations deems as acceptable and unacceptable use of its network.

2.3 Willful or negligent disregard of this policy may be investigated and dealt with under this Organizational Disciplinary Procedure.

2.4 This policy applies to all networks managed by The BAT used for:

- The storage, sharing and transmission of any confidential data and images;
- The storage, sharing and transmission of public data and images;
- Printing or scanning confidential or public data or images;
- The provision of Internet systems for receiving, sending and storing confidential or public data or images.

3 The Policy

3.1 The Network Security Policy for The Organization is described below:

The BAT's and its managed Organization's information network will be available when needed and can be accessed only by legitimate Users. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, The BAT will undertake the following:

a. Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures;
b. Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
c. Implement the Network Security Policy in a consistent, timely and cost-effective manner.
d. Where relevant, The Organization will comply with:

- Copyright, Designs & Patents Act 1911
- Information and Communication Technology Act 2006
- Digital Security Act 2018
- Computer Fraud and Abuse Act of 1986
- National Information Infrastructure Protection Act
- The Information Quality Act (P.L. 106-554).
- National Human Rights Commission Act, 2009
- Electronic Communications Act 2000
- Regulation of Investigatory Poours Act 2000
- The Right to Information Act 2009

b. The BAT will comply with other laws and legislation as appropriate.

4 Risk Assessment and audit

4.1 The BAT is responsible for ensuring that appropriate risk assessment(s) are carried out in relation to all the business processes covered by this policy. The risk assessment will identify the appropriate countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

4.2 Connecting for BAT Managed Organization's Information Governance Toolkit requires the BAT to undertake a self-assessment audit based on defined indicators.

4.3 Internal Audit has the ability to undertake an audit of compliance with policy on request.

5 Physical & Environmental Security

5.1 Core network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that has a monitored temperature and backup poour supply.

5.2 Core network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

5.3 Critical or sensitive network equipment will be protected from poour supply failures.

5.4 Critical or sensitive network equipment will be protected by fire suppression systems.

5.5 Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

5.6 All visitors to secure network areas must be authorised by a senior member of the technical support team.

5.7 All visitors to secure network areas must be made aware of security requirements.

5.8 All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.

5.9 The BAT will ensure that all relevant staff are made aware of procedures for visitors.

5.10 Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. BAT will maintain and periodically review a list of those with unsupervised access.

6 Access Control to the Network

6.1 Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
6.2 There must be a formal, documented user registration and de-registration procedure for access to the network. Separate authorisation will be required for Remote Access to the network.
6.3 The departmental manager must approve User access prior to being processed by the IT Service Desk.
6.4 Access rights to the network will be allocated on the requirements of the User's job, rather than on a status basis.
6.5 Security privileges (i.e. 'Superuser' or network administrator rights) to the network will be allocated on the requirements of the User's job, rather than on a status basis.
6.6 Users will be sent a Terms of Use agreement on application, which they must familiarise themselves with.
6.7 Access will not be granted until the Service Desk registers a user.
6.8 All Users to the network will have their own individual User identification and password.
6.9 Users are responsible for ensuring their password is kept secret (see User Responsibilities 25.2).
6.10 User access rights will, upon notification from departmental managers, be immediately removed or reviewed for those Users who have left **BAT** or changed jobs.

7 Remote Access

7.1 Remote Access refers to any technology that enables BAT to connect users in geographically dispersed locations.
7.2 **BAT** is responsible for ensuring that a formal risk assessment is conducted to assess risks and identify controls needed to reduce risks to an acceptable level.
7.3 **BAT** is responsible for providing clear authorisation mechanisms for all remote access users.
7.4 Head of The Departments are responsible for the authorisation of all applications for remote access and for ensuring that appropriate awareness of risks are understood by proposed Users.
7.5 All remote access users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources and notify **BAT** immediately of any security incidents and/or breaches.
7.6 Further information on 'mobile computing and communications' is available within the Agile Working Policy or from the Head of The Department – Information and Security Department.

7.7 **BAT** is responsible for ensuring that the Remote Access infrastructure is periodically reviewed, which could include but is not limited to independent third-party penetration testing.

8 Wireless Network

8.1 **BAT** has deployed a wireless network across many premises which is for the use of employees and authorised representatives only, to connect **BAT** owned IT equipment to the network.

8.2 The wireless network security standards are as follows:

a) Access Layer: Users will connect to the WLAN via Access Points, which will provide the 802.11a/b/g/n connection standard for the client devices.

b) Service Set Identifier (SSID2): The SSID for the staff access may be hidden and not broadcast thus reducing the potential for inappropriate access.

c) The SSID for 'guest' access to the Internet only, will be broadcast so as to make it easily available to authorised visitors. Access will be granted via the IT Service Desk.

d) Encryption: The wireless networks will utilise AES (Advanced Encryption Standard) level of encryption. This encryption standard is mandatory to enable the 802.11n network to be supported.

e) Authentication: The authentication protocol selected used is Protected EAP (PEAP). PEAP is an 802.1X authentication type for wireless networks.

f) The laptops used by **BAT** staff will confirm to the WPA 2 (Wi-Fi Protected Access) standard.

g) Unauthorised devices connected to the wireless network shall be blocked with no warning.

h) Staff should not attempt to connect personally owned wireless devices to **BAT** wireless network.

9 Third Party Access Control to the Network

9.1 Third party access to the network will be based on a formal contract that satisfies all necessary **BAT** security conditions.

9.2 The Information and Security Team is responsible for ensuring all third-party access to the network is logged.

9.3 Access to the internet may be provided for Other staff or **BAT** employed contractors via the Information and Security Department or IT Help Desk. Connection to the **BAT** Wi-Fi infrastructure may be approved where a senior BAT **Department Head** requests such access.

10 External Network Connections

10.1 **BAT** is responsible for ensuring that all connections to external networks and systems conform to the Code of Compliance and supporting guidance found in the Information Governance Toolkit.

10.2 **BAT** is responsible for ensuring all connections to external networks and systems are documented and approved by **BAT** before they commence operation.

11 Maintenance Contracts

11.1 **BAT** will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

12 Data and Software Exchange

12.1 Formal agreements for the exchange of data and software between organisations must be approved by the Proper Authority.

13 Fault Logging

13.1 **BAT** Information and Security Team is responsible for ensuring that a log of all faults on the network is maintained and reviewed. All log will be collected through central logging server.

14 Data Backup and Restoration

14.1 **BAT** is responsible for ensuring that backup copies of switch configuration and data stored on the network are taken regularly.
14.2 A log should be maintained of switch configuration and data backups detailing the date of backup and whether the backup was successful.
14.3 Documented procedures for the backup process will be produced and communicated to all relevant staff.
14.4 Documented procedures for the storage of backup tapes will be produced and communicated to all relevant staff.
14.5 All backup tapes will be stored securely and a copy will be stored off-site.
14.6 Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
14.7 Users are responsible for ensuring that they backup their own data to the network server.
14.8 Patches and any fixes will only be applied by The **BAT** following suitable change control procedure.

15 Malicious Software

15.1 **BAT** must ensure that measures are in place to detect and protect the network from viruses and other malicious software. In this case BAT and its Managed Organization will follow the Server_Anti_Malware_Policy_BAT document when needed.

16 Unauthorised software

16.1 Use of any non-standard software on **BAT** equipment must be approved by Information and Security Team before installation. All software used on **BAT** equipment must have a valid licence agreement - it is the responsibility of the Information Asset Owner or Responsible User of non-standard software to ensure that this is the case.

17 Secure Disposal or Re-use of Equipment

17.1 **BAT** must ensure that where equipment is being disposed of all data on the equipment (e.g. on hard disks or tapes) is physically destroyed prior to leaving this Organization premises for disposal.

17.2 The **BAT** must ensure that where electronic media are to be removed from the premises for repair, where possible, the data is securely overwritten.
For advice please contact the Head of The Department – Information and Security.

18 System Change Control

18.1 The **BAT** is responsible for ensuring that appropriate change management processes are in place to review changes to the network; which would include acceptance testing and authorisation. The BAT is responsible for ensuring all relevant Network documentation is up to date.

18.2 BAT is responsible for ensuring that selected hardware or software meets agreed security standards.

18.3 Testing facilities will be used for all new network systems. Development and operational facilities should be separated.

19 Security Monitoring

19.1 **BAT** is responsible for ensuring that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

19.2 **BAT** reserves the right to access, modify or delete all data stored on or transmitted across its network. This includes data stored in personal network folders, mailboxes etc. Data of a personal nature should be stored in a folder marked or called 'Private'. This does not preclude access or removal of such a folder on the authority of Head of Information and Security Team.

19.3 **BAT** reserves the right to disconnect or block any device connected either by physical or wireless means to the network.

19.4 **BAT** reserves the right to block any physical non-approved device connected to a piece of **BAT** owned equipment.

20 Training and Awareness

20.1 Head of Information and Security Team will work in conjunction with the IT Trainers to provide security awareness training for all staff to ensure that they are aware of their responsibilities for security, and the actions that they need to undertake in order to discharge those responsibilities.

20.2 All users of the network must be made aware of the contents and implications of the Network Security Policy.

21 Reporting Data Security Breaches and Weaknesses

21.1 Data Security Breaches and weaknesses, such as the loss of data or the theft of a laptop, must be reported in accordance with the requirements of the **BAT** 's incident reporting procedure and, where necessary, investigated by the Information and Security Team.

22 System Configuration Management

22.1 **BAT** will ensure that there is an effective configuration management process for the network.

23 Disaster Recovery Plans

23.1 **BAT** will ensure that disaster recovery plans are produced for the network and that these are tested on a regular basis.

24 Unattended Equipment and Clear Screen

24.1 Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.

24.2 **BAT** operates a clear screen policy that means that Users must ensure that any equipment logged on to the network must be protected if they leave it unattended,

even for a short time. Workstations must be locked or a screensaver password activated if a workstation is left unattended for a short time.

24.3 Users of dumb terminals must log out when not using the terminal.

25 Responsibilities

25.1 Information and Security Department Responsibilities

25.1.1 Act as a central point of contact on network security within the organisation, for both staff and external organisations.

25.1.2 Implement an effective framework for the management of network security.

25.1.3 Assist in the formulation of Network Security Policy and related policies and procedures.

25.1.4 Advise on the content and implementation of the relevant action plans.

25.1.5 Produce organisational standards, procedures and guidance on Network Security matters for approval by **BAT**. All such documentation will be included in the Asset register.

25.1.6 Co-ordinate network security activities particularly those related to shared information systems or IT infrastructures.

25.1.7 Liaise with external organisations on network security matters, including representing the organisation on cross-community committees.

25.1.8 Create, maintain, and give guidance on and oversee the implementation of network security.

25.1.9 Represent the organisation on internal and external committees that relate to network security.

25.1.10 Ensure that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.

25.1.11 Ensure the systems, application and/or development of required policy standards and procedures in accordance with business needs, policy and guidance.

25.1.12 Ensure that access to the organisation's network is limited to those who have the necessary authority and clearance.

25.1.13 Provide advice and guidance to development teams to ensure that the policy is complied with.

25.1.14 Approve system security policies for the infrastructure and common services.

25.1.15 Approve tested systems and agree plans for implementation.

25.1.16 Advise on the accreditation of IT systems, applications and networks

25.1.17 Ensure that Network Security is included within the **BAT** Mandatory training programme.

25.1.18 Support incident assessments, where necessary

25.1.19 Provide support on user matters relating to Network Security

25.1.20 Ensure the security of the network, (that is information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements and obligations.

25.1.21 Ensure that staff are aware of their security responsibilities.

25.1.22 Ensure that staff have had suitable security training.
25.1.23 Ensure that the IT Service Desk is promptly notified when new accounts are required.
25.1.24 Ensure that the IT Service Desk is promptly notified when existing accounts are to be reviewed or deleted, e.g. when a member of staff changes roles or leaves the organisation.

25.2 User Responsibilities

All personnel or agents acting for the organisation have a duty to:

25.2.1 Safeguard hardware, software and information in their care.
25.2.2 Prevent the introduction of malicious software on the organisation's IT systems.
25.2.3 Users are responsible for ensuring their password is kept secret - ***passwords should not be shared under any circumstances.***
25.2.4 Passwords should be changed regularly and be such that they are not easily guessed e.g. names of relatives or pets. Network passwords must:
a) be changed every 60 days
b) not contain the user's network account name or parts of the user's full name that exceed two consecutive characters
c) be at least 8 characters in length
d) contain characters from three of the following four categories:
i. English uppercase characters (A through Z)
ii. English loourcase characters (a through z)
iii. base 10 digits (0 through 9)
iv. non-alphabetic characters (for example, !, $, #, %)
25.2.5 If a user suspects that their network password has become compromised, they should report this to the Information Security Team and change their password.
25.2.6 Report on any suspected or actual breaches in security.

25.3 SIRO Responsibilities

The Senior Information Asset Risk Owner is responsible for:

25.3.1 Planning for information security by setting an overall Network Security Policy for the organisation.
25.3.2 Meeting the legal requirement and ensuring that operational compliance is further delegated to the Information Asset Owners.
25.3.3 Ensuring that, where appropriate, staff receive Information Security awareness training.
25.3.4 Ensuring that the network is risk assessed and any risks identified either mitigated or escalated

26 Further information

26.1 If you would like any further information regarding this policy please do not hesitate to contact Information and Security Team.
If you do not have any questions, BAT presumes that you understand and are aware of the rules and guidelines in this Internet Use Policy and will adhere to them.

27 Development of Procedural Document

27.1 Prioritisation of work

This document has been developed so that all employees are aware of the associated information technology requirements within the organisation in a consistent manner, ensuring that new employees are practicing in a way that ensures best practice.

27.2 Consultation and Communication with Stakeholders

This policy and subsequent programme was developed in consultation with a number of staff focus groups and in conjunction with Business Automation Ltd as well as partner and clients of BAT who share a common local area network infrastructure.

27.3 Approval of policy

- The director lead for this policy is the CEO, the responsibility for the development has been delegated to Head of Information and Security.
- The Management Team is responsible for the final approval of this policy
-

27.4 Identification of Stakeholders

Stakeholder	**Level of involvement**
Management Team	Consultation, final approval
Extended Executive Management Team	Allocated lead, development, consultation, receipt, circulation
Information and Security Team	Dissemination, implementation, monitoring

28 Document control and archiving

28.1 Will be available on the intranet in read only format.

28.2 A central electronic read only version will be kept by the Integrated Governance Manager in a designated shared folder to which all Executive Management Team members and their administrative staff have access.

28.3 A central paper copy will be retained to HR Department.

IT Access & User Management Policy

Document Control

Organisation	Business Automation Ltd.
Title	IT Access & User Management Policy
Author	Md. Shiful Islam
Filename	IT Access Policy BAT
Owner	Head of Information Security
Subject	User Access Control
Protective Marking	[Marking Classification]
Review date	

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contributors

Development of this policy was assisted through information provided by the following Department:

- Information Security Department
- Software Development Department
- Management Department
- Implementation and Support Department
- Application Department

1 Policy Statement

Business Automation Ltd. will establish specific requirements for protecting information and information systems against unauthorised access.

Business Automation Ltd. will effectively communicate the need for information and information system access control.

Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Business Automation Ltd. which must be managed with care. All information has a value to the Organization. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

Scope

This policy applies to all Business Automation Ltd. Councillors, Committees, Departments, Partners, Employees of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Organization with any form of access to Business Automation Ltd.'s information and information systems.

Definition

Access control rules and procedures are required to regulate who can access Business Automation Ltd. information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Business Automation Ltd. information in any format, and on any device.

Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the Organization and may result in financial loss and an inability to provide necessary services to our customers**.**

Applying the Policy – Passwords and User Authentication

Choosing Passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Weak and *strong* passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Password Requirements in General

- For every new user there will be a temporary password which must be changed after first login.
- Passwords shall have a minimum of 8 characters with a mix of alphanumeric and special characters, if a particular system will not support 8-character passwords, then the maximum number of characters allowed by that system shall be used.
- Passwords shall not consist of well-known or publicly posted identification information. Names, usernames such as the MyID, and ID numbers such as the 81x or UGAID number are all examples of well know identification information that should not be used as a password.
- Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames. Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.
- Users will be prohibited from re-using the last 5 previously used passwords.
- Care shall be taken to prevent the compromise of one username/password from compromising the security of multiple systems or resources. The username and password(s) used for your UGA accounts should never be used for any other non-UGA accounts and services.
- Passwords shall not be transferred or shared with others unless the user obtains appropriate authorization to do so.
- Passwords shall not be transferred electronically over the Internet using insecure methods. Wherever possible, security protocols including IMAPS, FTPS, HTTPS, etc. shall be used.

Additional Password Requirements for System Administrators

- Require Passwords for Login - Systems shall not be configured to allow user login without a password. Exceptions shall be granted for specialized devices such as public access kiosks when these devices are configured with public user accounts that have extremely restricted permissions (e.g. web only) that are separate from administrative accounts.
- Protect Against Password Hacking - System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate “brute force” password attacks. For example, some systems will lock an account for a few minutes after several failed login attempts or detect where the attack is coming from and block further attempts from that location, or at minimum alert an alert in real-time that an attack is underway so that manual action can be taken.
- Logging - Practicable measures shall be put in place to log successful and failed login attempts.

- Changing Password after Compromise or Disclosure - System administrators shall, in a timely manner, reset passwords for user accounts or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource. Examples of these situations include but are not limited to: disclosure of a password to an unauthorized person; discovery of a password by unauthorized person; system compromise (unauthorized access to a system or account); insecure transmission of a password; replacing the user of an account with another individual requiring access to the same account; password is provided to IT support staff in order to resolve a technical issue; account password is communicated to a user by the system administrator.
- Default Passwords - System administrators shall not use default passwords for administrative accounts.

Additional Password Requirements for Application Developers

- Require Secure Transmission - Application developers shall, whenever possible, develop applications that require secure protocols for authentication.
- Storing Passwords - Application developers shall avoid creating applications which store passwords. If password storage cannot be avoided, application developers shall ensure that applications do not store passwords in clear text or an easily decrypted format.
- Unique User Accounts and Passwords - Applications shall support unique user accounts and passwords so that individual users are not required to share a password in order to use the application.

- Use team specified and Password Whenever Possible - Applications shall, whenever capable, use the team specified ID and its associated password for authenticating members of that team instead of creating another unique ID or username.

Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Business Automation Ltd. systems.
- Do not use the same password for systems inside and outside of work.

Changing Passwords

All user-level passwords must be changed at a maximum of every 60 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to Information Security Department.

Users **must not** reuse the same password within 10 password changes.

User Authentication Policy

Account Lockout Policy

Another possible defence against password-guessing attacks is enabling an account-lockout policy, which means the account will be locked after a specified number of invalid or failed login attempts.

- Account lockout duration: 60 minutes
- Account lockout threshold: 5 invalid logon attempts
- Reset account lockout after: 0 minutes [account does not unlock automatically]
- System Admin will reserve the poour to lockout the locked account after proper approval immediately.

Session Lockout Policy

A logged in user session will be automatically log out after 30 minutes of the user's idle time.

Applying the Policy – Employee Access

User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by Business Automation Ltd. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

User Registration

A request for access to the Organization's computer systems must first be submitted to the respective department for approval. Applications for access must only be submitted if approval has been gained from respective **Line Manager**.

When an employee leaves the Organization, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the respective **Line Manager** to request the suspension of the access rights via the **Information Security Department** of Business Automation Ltd.

User Responsibilities

It is a user's responsibility to prevent their userID and password being used to gain unauthorised access to Organization systems by:

- Following the Password Policy Statements outlined above in Section 6.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing his/her **Line Manager** and **Information Security Department** of any changes to their role and access requirements.

Network Access Control

The use of modems on non-Organizational owned PC's connected to the Organization's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from **Information Security Department** before connecting any equipment to the Organization's network.

User Authentication for External Connections

Where remote access to the Business Automation Ltd. network is required, an application must be made via the **Line Manager** to **HOD** of **Implementation** and **Information Security Department**. Remote access to the network must be secured by remote logging server.

Supplier's Remote Access to the Organization Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from **Information Security Department**. Any changes to supplier's connections must be immediately sent to the **Information Security Department** so that access can be updated or ceased. All permissions and access methods must be controlled by **Information Security Department.**

Partners or 3rd party suppliers must contact the **Information Security Department** before connecting to the Business Automation Ltd. network and a log of activity must be maintained. Remote access software must be disabled when not in use.

Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 7.1) and the Password section (section 6) above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The respective Owner or Administrator of the software application is responsible for granting access to the information within the system. The access:

- Be compliant with the User Access Management section (section 7.1) and the Password section (section 6) above.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

Policy Compliance

If any user is found to have breached this policy, they may be subject to Organization's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from **Information Security Department**.

Policy Governance

The following table identifies who within Business Automation Ltd. is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Head of Information Services - **Md. Shiful Islam** Head of Implementation and Support – **Md. Mithu Pramanik** Head of Human Resources - **A. K M. Ahsanul Kabir**

Accountable	Managing Director - **Mr. Jahidul Hasan**
Consulted	Information and Security Department Implementation and Support Department Application and Testing Department Application Development Department Company Management Unit
Informed	All Organization Employees All Temporary Staff All Contractors All Vendors who need access

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by **Mr. Jahidul Hasan**, CEO of Business Automation Ltd.

References

The following Business Automation Ltd. policy documents are directly relevant to this policy, and are referenced within this document [amend list as appropriate]:

- Remote Working Policy.
- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- Acceptable Usage Policy and Personal Commitment Statement.
- Legal Responsibilities Policy.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Information Protection Policy.

- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- IT Infrastructure Policy.
- Communications and Operation Management Policy.

Key Messages

- All users must use **strong** passwords.
- Passwords must be protected at all times and must be changed at least every 60 days.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their userID and password being used to gain unauthorised access to Council systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Organization's network without permission from **Information Security Department**.
- Partners or 3rd party suppliers must contact the **Information Security Department** before connecting to the Business Automation Ltd. network.
- Appendix 1

[Include any relevant associated information within appendices. This may include any templates or forms that need to be completed as stated within the policy]

1. BAT_UserAccessRequestForm_Form 01-001F

Disaster Recovery Teams & Responsibilities

In the event of a disaster, different teams will be required to assist the IT department in their effort to restore normal functionality to the employees of Business Automation Ltd & our consortium partner. The different teams and their responsibilities are as follows:

- Disaster Recovery Lead(s)
- Disaster Management Team
- Network Team
- Server Team
- Applications Team

Disaster Recovery Lead

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at Business Automation Ltd & our consortium partner, regardless of their department and existing managers. All efforts will be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased. As a result, the Disaster Recovery Lead will not be a member of other Disaster Recovery groups in Business Automation Ltd.

Roles & Responsibilities

- Make the determination that the organization is declaring that a disaster has occurred and trigger the DR Plan and related processes.
- Initiate the DR Notification Network.
- Be the single point of contact for and oversee all of the DR Teams.
- Organize and chair regular meetings of the DR Team leads throughout the disaster.
- Present to the Management Team on the state of the disaster and the decisions that need to be made.
- Organize, supervise and manage all DR Plan test and author all DR Plan updates.

Contact Information

Name	Role	Work Phone	Home Phone	Mobile Phone

Management Team

Roles & Responsibilities

- Set the DR Plan into motion after the Disaster Recovery Lead has declared a disaster
- Determine the magnitude and class of the disaster
- Determine what systems and processes have been affected by the disaster
- Communicate the disaster to the other disaster recovery teams
- Determine what first steps need to be taken by the disaster recovery teams
- Keep the disaster recovery teams on track with pre-determined expectations and goals
- Keep a record of money spent during the disaster recovery process
- Ensure that all decisions made abide by the DR Plan and policies set by Business Automation Ltd
- Get the secondary site ready to restore business operations

- Ensure that the secondary site is fully functional and secure
- Create a detailed report of all the steps undertaken in the disaster recovery process
- Notify the relevant parties once the disaster is over and normal business functionality has been restored
- After Business Automation Ltd. is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Contact Information

Name	Role	Work Phone	Home Phone	Mobile Phone

Network Team

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the organization as well as telephony and data connections with the outside world. They will be primarily responsible for providing baseline network functionality and may assist other IT DR Teams as required.

Roles & Responsibilities

- In the event of a disaster that does not require migration to / from Business Automation availability zones, the team will determine which network services are not functioning at the primary availability zones
- If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.
- If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.
- In the event of a disaster that does require migration to Business Automation availability zones the team will ensure that all network services are brought online at the secondary availability zones
- Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:
    - All members of the DR Teams
    - All Managers and Executive Staff
    - All IT employees
    - All remaining employees
- Install and implement any tools, hardware, software and systems required in the standby availability zone

- Install and implement any tools, hardware, software and systems required in the primary availability zone
- After Business Automation Ltd. is back to business as usual, this team will be summarizing any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.

Contact Information

Name	Role	Work Phone	Home Phone	Mobile Phone

Server Team

The Server Team will be responsible for providing the physical server infrastructure required for the organization to run its IT operations and applications in the event of and during a disaster. They will be primarily responsible for providing baseline server functionality and may assist other IT DR Teams as required.

Roles & Responsibilities

- In the event of a disaster that does not require migration to / from Business Automation availability zones, the team will determine which servers are not functioning at the primary availability zone
- if multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the following tasks:
    - Assess the damage to any servers
    - Restart and refresh servers if necessary
- Ensure that secondary servers located in Business Automation availability zones are kept up-to-date with system patches
- Ensure that secondary servers located in Business Automation availability zones are kept up-to-date with application patches
- Ensure that secondary servers located in Business Automation availability zones are kept up-to-date with data copies
- Ensure that the secondary servers located in the standby availability zones are backed up appropriately
- Ensure that all of the servers in the standby availability zones abide by Business Automation Ltd.'s server policy
- Install and implement any tools, hardware, and systems required in the standby availability zones
- Install and implement any tools, hardware, and systems required in the primary availability zones

- After Business Automation Ltd is back to business as usual, this team will be summarizing any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Contact Information

Name	Role	Work Phone	Home Phone	Mobile Phone

Applications Team

The Applications Team will be responsible for ensuring that all organization applications operate as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other IT DR Teams as required.

Roles & Responsibilities

- In the event of a disaster that does not require migration to / from Business Automation availability zones, the team will determine which applications are not functioning at the primary availability zones
- If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:
    - Assess the impact to application processes
    - Restart applications as required
    - Patch, recode or rewrite applications as required
- Ensure that secondary servers located in Business Automation availability zones are kept up-to-date with application patches
- Ensure that secondary servers located in Business Automation availability zones are kept up-to-date with data copies
- Install and implement any tools, software and patches required in the standby availability zones
- Install and implement any tools, software and patches required in the primary availability zones
- After Business Automation Ltd. is back to business as usual, this team will be summarizing any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Contact Information

Name	Role	Work Phone	Home Phone	Mobile Phone

Anti-Malware Policy

Version 1

Owner: Information and Security Team

Business Automation Ltd.

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
1	December 2018	Md. Shiful Islam	New Policy

Review Distribution

Name	Title
Md. Shiful Islam Sabuj	Head of Information and Security
Md. Mithu Pramanik	Head of Implementation and Support

Approval

Name	Position	Signature	Date
Mr. Jahidul Hasan	CEO		

1. Introduction

1.1

The Business Automation Ltd. (referred to hereafter as the BAT) is obliged to make sure its IT systems and other facilities are secured and not subject to improper use. This Policy sets out the responsibilities of all users, including users of privately-owned devices that connect to the BAT IT facilities, in relation to malicious software. These measures do not guarantee security, but they will help to significantly reduce the risk of widespread virus infection at the BAT.

1.2

The word 'malware' is used collectively to denote many types of malicious software, including viruses, ransomware, worms, trojans, macros, mail bombs and rootkits.

A virus is a piece of self-replicating computer program code that is designed to destroy or damage digital information, or to steal user or business data.

1.3

There are many potential sources of malicious software, including websites, social media, USB memory sticks, unsolicited CDs, electronic mail, and software or documents copied over networks such as the campus network or the internet.

1.4

A malware infection is costly to the BAT and often time-consuming for individuals. This may be through the loss of data or access to IT systems, staff time to recover a system, or the delay or loss of important work. Additionally, malicious software can spread from an infected system and can lead to severe disruption to IT services and possible reputational damage or even fines. Malicious software is a constantly evolving threat and the BAT therefore applies controls to protect our systems and information from all forms of malware.

2. Scams and Hoaxes

2.1

Many spam emails are sent with dire warnings about messages with topical subjects or attachments. The receiver is often asked to forward the email to all colleagues and friends around the globe. If you are unsure whether an email you receive is a hoax or scam, you can check it at https://tools.verifyemailaddress.io

Do not forward these messages on. If you receive such a message, just delete it.

2.2

Some websites you visit will suggest your PC or tablet is infected with a new virus and hence you need to run / install / purchase their anti-virus software.

Do not click this message. Instead, check that you have the latest signatures and updates in your existing anti-virus software and then run a manual scan.

2.3

If you download a fake anti-virus application, or think that your device has a virus, please report this to the Information and Security Team as soon as possible, because it will be much easier to remove if reported promptly.

3. Scope

3.1

This Policy applies to all users, including Guest users and other users of privately-owned devices that connect to the BAT IT facilities. By following this Policy, users will help to protect themselves and other BAT users against malicious software. The BAT IT Regulations, on which this Policy expands, require everyone to take the practical steps needed to keep this protection active and up to date. If in doubt, contact the Information and Security Department on sabuj@batworld.com extension 123 Or 01711163535.

4. Purpose

4.1

The objectives of this document are:

- To set out user responsibilities about malicious software prevention
- To set out the rules governing the application and use of malicious software prevention systems at the BAT.

5. Policy

- All BAT personal computers and servers that are connected to the BAT network or otherwise using the IT facilities must run an approved and up-to-date anti-malware product that continually monitors for malicious software (viruses, worms, etc.).
- All personal computers, devices and servers connected to the BAT network must run a supported version of the Operating System and installed applications with the latest available patches applied.
- Computers and tablets supported by Academic Services will be supplied with an anti-malware product with automatic updating for it and for the Operating System and applications.
- Any non-BAT owned devices must run an appropriate anti-malware product. Details of suitable products can be found at www.exeter.ac.uk/it/virusesandmalware
- Users who do not choose a recommended anti-malware product must make their own adequate anti-malware protection arrangements for their privately-owned devices that meets the requirements described here.
- Anti-malware must be configured for on-access scanning, including the downloading or opening of files, folders on removable or remote storage, and web page scanning.
- Anti-malware protection software must be configured to run regular (at least daily) scans.
- Users must be prevented from accessing known malicious web sites either by malware protection software or through a content filtering function.
- Do not try to uninstall or disable anti-virus software. Any messages suggesting that anti-virus protection has been disabled should be investigated immediately.
- If users experience difficulties with a recommended anti-virus product, requests for technical support may be made through the helpdesk.
- The BAT's IT Regulations prohibit any activity intended to create and / or distribute malicious code (viruses, worms, etc) on the BAT network or IT facilities. However, when requested to do so by Exeter IT staff in order to aid investigations, users may send suspected malware using a method that does not allow the malware to propagate / spread.
- The BAT reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.
- If you suspect that a device is infected with a virus, report the incident to the helpdesk and / or to local IT staff as soon as possible.
- Email attachments must be scanned by an anti-virus product before delivery.
- Check the authenticity of attachments / software to be installed from internet sources. Do not install applications that arrive on unsolicited media.

Individuals may be subject to disciplinary action if this Policy is breached.

Management and Migration of Legacy Data

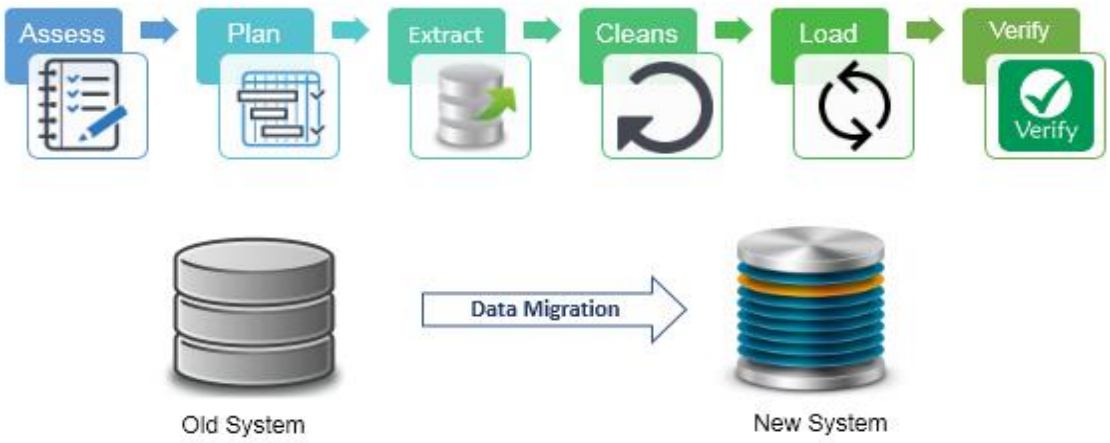
As BUSINESS AUTOMATION is currently using a system so it is important to migrate the data from the old system to the new system. The data migration will be done in several steps. The management and migration data will follow below process/activities for migrating data.

For planning we will perform a mapping to migrate the data. A mapping document will be prepared the document will consists.

- Change Description
- Key indicator
- Source field Name
- Source Table/File Name
- Source Field Data Type
- Source Field Length
- Source Field Description
- Business Role
- Target Table Name
- Target Field Name
- Target Data Type
- Target Field Length
- Comments

The management and migration data will follow below process/activities for migrating data.

Fig: Data migration Process



On Data Extraction phase we will identify data extracted in System Discovery phase then export features of the source system used. After exporting features, we will generate scripts to export the data.

On data cleansing phase at first, we will detect incomplete parts of data. Modifies / Eliminates inaccurate records.

On load phase we will work on 3 steps. They are

- Load
- Update
- Schedule

Data verification steps are given below:

- Checking table row count
- Monitor Database integrity
- Check impacts on the operational performance
- Test using the subset of data
- Testing translation rules implementation
- Involves testing for data type conversions

Documentation Plan

Expected Deliverables

Considering the scope of the service and scope of work of this project and based on the proposed project development & implementation methodology we will submit below deliverables within the project timeline:

- Project Inception and Management Report
- System Requirement Specification (SRS)
- System Design Document (SDD)
- Complete Source Code
- Detail Source Code Documentation
- Test Plan with test scripts and testing reports
- Training Plan & Reports
- Maintenance agreement & SLA
- Maintenance and support log
- Hosting requirement specification, plan and report
- HR activity plan and report
- Monthly Progress report
- Progress and review reports

Before go through with a report, we must first know where our organization or projects are in the risk lifecycle.

Risk and manifestation change as security programs and specific IT projects mature. Risk expressively increases as projects and organizations move through the strategic, technical and operational stage.

Every organization will have different business cultures, operations and expectations. These variables will greatly influence how executives will want to receive security information and

reports. It’s important to understand our business's culture, goals and priorities, and align our security thinking and reporting to them. Additionally, a comprehensive security report that bridges the three stages can be used to show how ongoing security initiatives and blame are affecting later phases of a project or ongoing operations.

By extrapolating data from the assessment and activity reports across multiple projects and departments, we can identify ensure aptitude that can show cascading security issues, and forecast future security problems

For instance, spikes in virus infections in certain departments could indicate a failure to update AV signatures. Or, an abnormally high number of password-reset requests could indicate an overly stringent password policy.

So we need to able to protect ourselves from cyber related attack.