Cyber Security Byelaw, 2077 (2020)

In exercise of the powers conferred by Section 62 of the Telecommunication Act, 2053 (1997) Nepal Telecommunications Authority (NTA) has framed this Byelaw for the implementation of cyber security standards and best practices so as to protect ICT Infrastructure and Information Systems of Telecommunication Service Providers of Nepal from various malicious attacks and threats; and build trust and confidence of users towards using ICT technology and services.

Chapter-1

Preliminary

1. **Short Title and Commencement:** (1) This Byelaw is called as the "Cyber Security Byelaw, 2077 (2020)".

   (2) This Byelaw shall come into force immediately.

2. **Definitions:** Unless the subject or context otherwise requires, in this Byelaw,-

   (i) "Act" means the Telecommunication Act, 2053 (1997).

   (ii) "Regulation" means the Telecommunication Regulation, 2054 (1998).

   (iii) "Authority" means Nepal Telecommunications Authority (NTA) established under the Telecommunication Act, 2053 (1997)

   (iv) "Licensee" means the telecommunications service providers who have obtained license from NTA.

   (v) **"**Denial of Service (DoS) Attack**"** means overloading a system with so many requests so that it cannot serve normal requests.

   (vi) **"**Identity theft**"** means pretending to be someone you are not.

   (vii) **"**Fraud**"** means manipulating data for the purpose of committing a crime, e.g. changing financial records to enable someone steal or transfer money to an account.

   (viii) "Spamming" means distributing unsolicited e-mails to hundreds of different addresses.

   (ix) "Intellectual property theft" means stealing of another person's or companies intellectual property.

   (x) "Phishing" means deceiving individuals to gain private or personal information about them.

(xi) “Spoofing” means pretending to be something else in an attempt to gain confidence, get access to a system, steal data or spread malware.

(xii) “Unauthorized access” means gaining access to systems you are no authority or have no permission to access.

(xiii) “Core Services” means the services which includes but not limited to the exposed services to the public internet such as Web, Email, Domain Name System (DNS), Billing, Customer Relationship Management (CRM) etc.

(xiv) “Core System” means the system which provides core services.

(xv) “Cloud Services” means services that provide on-demand availability of computer system resources and services, especially data storage (cloud storage) and computing power, without direct active management by the user.

(xvi) “Critical Services” means the services identified as critical by the licensee.

(xvii) “Next Generation Firewall” means Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.

(xviii) “IP” means Internet Protocol based on Version 4 and Version 6.

(xix) “Sensitive Data” means the data which includes but not limited to password, phone number, email address, mobile number, card number, PIN, security code, bank details etc.

(xx) “Critical Emergency Response Team (CERT)" means an expert group that handles computer security incidents.

(xxi) “Security Operation Center (SOC)" means a team and a facility dedicated to and organized to prevent, detect, assess and respond to cyber security threats and incidents, and to fulfill and assess regulatory compliance.

(xxii) “Route Origin Authorization (ROA)” means a digitally signed object that provides a means of verifying that an IP address block holder has authorized an Autonomous System (AS) to originate routes to one or more prefixes within the address block.

(xxiii) “Resource Public Key Infrastructure (RPKI)” means an Infrastructure to Support Secure Internet Routing that includes cryptographic method of signing records that associate a BGP (Border Gateway Protocol) route announcement with the correct originating AS number.

(xxiv) “AAA” stands for Authentication, Authorization and Accounting.

Chapter-2

Provisions Relating to General Security Standards and Practices

3. Licensee shall have an updated recorded copy of document where all its technological assets like hardware, software, and license are managed and segregated as per criticality, usage, location, versions, owner, purchase date, update date like details.

4. Licensee shall have its board approved ICT Security Policies for planning, organizing, directing, controlling and monitoring of information management systems. These ICT Security Policies shall be applied/ executed for efficient and effective management of People, Process and Technology.

5. Licensee shall review ICT Security Policies developed at least once a year. However such policies can also be reviewed frequently as per the need or as per major changes in organizational structure, infrastructure or process.

6. Licensee shall have clearly defined and updated organogram with roles and responsibilities for its personnel (system operators, system developers, network administrators, information owners, security officers, users etc.), which shall be reviewed periodically.

7. Licensee shall have employees' related policy addressing the following items.
   (i) Proper handling of social media.
   (ii) Usage of Official Devices.
   (iii) Usage of Personal devices.
   (iv) Proper handling of official emails/accounts and information.

8. Licensee shall have provision for access control and proper segregation of dedicated computing environment for highly sensitive systems. Also, Access controls shall be configured to ensure that users are restricted to Read, Write, Execute, Delete based on the organizational information access policy.

9. Licensee shall promote information security awareness throughout the organizations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and confirm to security best practices.

10. Licensee shall adopt risk-based approach to identify, prioritize and address the security risks and consequences associated with vulnerabilities of information systems in a consistent and effective manner and determine the mitigation measures to reduce the risks to an acceptable level.

11. Licensee shall have provisions for User Account and in general comply with the followings:

    (i) All user accounts and their privileges should be subject to an approval process and should be documented.

    (ii) Admin privileges and any other special access privileges should be restricted to authorized individuals and documented.

    (iii) Admin accounts shall only be used to perform admin tasks and not for everyday access.

    (iv) Admin accounts shall be set to require a password change every ninety (90) days or less.

    (v) Every individual user shall have a unique user name and user account.

    (vi) Any user account with special privileges or admin rights shall be removed or periodically disabled when no longer required or if the individual changes role or leaves the organization or after a predefined length of inactivity (e.g. if the account is not used for ninety days then it is disabled).

12. Licensee shall enforce the following rules in organization for implementing password policy:

    (i) Password shall be at least ten (10) characters long.

    (ii) Password shall include combination of upper case- and lower-case alphabets, numbers and special characters.

    (iii) Password shall not be same as user name.

    (iv) Password shall not be a dictionary word.

    (v) Password does not contain any identical characters next to each other

    (vi) Same Passwords shall not be used for multiple accounts in different platforms.

    (vii) Passwords shall be reused within a predetermined time period.

    (viii) The default password on the device shall be changed from the default to an alternative strong password.

    (ix) Passwords shall be changed after every ninety (90) days periodically.

    (x) Already used passwords shall not be used while changing passwords.

13. Licensee shall act proactively as a first line of defense to protect their customers from known attacks and for this they shall

    (i) Recommend tools/solutions (may include Anti-virus, antispyware, anti spam, malware protection, firewall provision, advise on backup of data, identity protection etc) to protect from the possible threats via available means of communication.

(ii) Detect threats/malware/botnets based on IP addresses of customers and inform them for cleaning their devices.

14. Licensee shall use commercial licensed Operating System (OS), applications, antivirus/antimalware used in Servers, Desktop, Laptop and Mobile devices etc.

15. Licensee shall follow the common best security practices defined by SANS, CIS etc. while using open source such as GNU General Public License, BSD license for operating system, applications, antivirus/antimalware etc.

16. Licensee shall perform regular update of Antivirus, Database, Application Libraries, Operating System, Kernel etc.

17. Licensee shall restrict default login for any applications, systems or software.

18. Licensee shall make provision for closing all hardware ports (including USB, CD/DVD and External Devices) of the devices (servers) for discouraging copying files directly and use alternative methods of sharing files like file server.

19. Licensee shall make provision for using Centralized Authentication System like Active Directory (AD), Light Weight Directory Access Protocol (LDAP) for AAA of its employees.

20. Licensee shall be encouraged to use PGP/Digital signature in email communications, documents, letters and other applications.

21. Licensee shall bind manufacturers/vendors/suppliers of hardware, software and related infrastructure to patch the vulnerabilities ensuring minimum level of security.

22. Licensee shall make use of national and international cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

23. Licensee shall have its board approved disaster recovery and Business Continuity Policy/Procedure/Plan (BCP) to counteract interruptions to business activities and to protect critical business processes from the effects of major failure or disaster:

(i) Redundancy and fault tolerance shall be built into the systems to minimize the impact of attacks and data corruption.

(ii) The BCP shall contain identification of attacks and security breaches, incident response plan, communication plan and escalation matrix.

(iii) The BCP shall contain offsite location for backups and disaster recovery.

24. Licensee shall establish security perimeters to protect physical and IT assets. Licensee shall establish protected entry controls, such as the followings, to ensure that only authorized personnel are allowed access:

(i) Badges,

(ii) Limited access to buildings,

(iii) Guards on entrance doors,

(iv) Properly secured and tamper proof wiring,

(v) Alarm doors.

Chapter-3

Provisions Relating to Infrastructure/Network Security

25. Licensee shall use DDoS Detection and Mitigation system to avoid possible DDoS attack on the network infrastructure.

26. Licensee shall have Flow Analyzer which shall be continuously monitored for threat intelligence (threat detection and alarming).

27. Licensee shall strictly use secure Virtual Private Network (with IPSec or SSL) when accessing the system remotely.

28. Licensee shall map and analyze organizational communication and data flows for possible security threats.

29. Licensee shall deploy Mutually Agreed Norms for Routing Security (MANRS).

30. Licensee shall have provision to securely authenticate users (2 Factor Authentication/ OTP) and provide encrypted access (IPSec/SSL) to Value Added Service Provider/Third Party into the core system to avoid any security risk.

31. Licensee shall:

(i) Perform Penetration testing of Critical infrastructure regularly.

(ii) Identify status of equipment performing vulnerability assessment.

(iii) Implement standard security configuration policy on Switches & Routers.

(iv) Isolate and segregate (VLAN) the networks based on needs.

32. Licensee shall routinely assess their suppliers/third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting their contractual security obligations.

33. Licensee shall implement Wireless Local Area Network (WLAN) security standards like WPA-2/3.

34. Licensee shall have Network Firewall and following shall be implemented:

(i) Firewall shall protect their internal network and devices against unauthorized access.

(ii) Each rule set on the firewall must be approved by an authorized individual and documented including an explanation of the business need of this rule.

(iii) Unapproved or vulnerable services should be blocked at the gateway firewall.

(iv) Any permissive firewall rules that are no longer required should be disabled as soon as possible.

(v) The firewall's boundary administration settings should not be accessible from the internet.

35. For secure Network, licensee shall adopt following security measures.

(i) All unnecessary user accounts, guest or admin accounts shall be removed or disabled.

(ii) All network infrastructure configurations shall be automatically backed up.

(iii) All auto-run and unused features shall be disabled.

(iv) Rogue Endpoints must be isolated.

36. Licensee shall ensure implementation of minimum set of configurations for hardening network and infrastructure identified in different standards like CIS, ISO, SANS, COBIT etc.

Chapter-4

Provisions Relating to Core System Security

37. Licensee shall use Next Generation Firewall to protect Core Service System from any form of vulnerability and attack and shall restrict access to default login.

38. Licensee shall frequently revisit and update firewall policy, close unnecessary ports, define max-failed-tries-within-time-limit for saving from Brute-force attack on Remote-access ports.

39. Licensee shall have provisions for IP block listing/allow listing, Port-Knocking based on needs.

40. Licensee shall have its public facing systems and services in public Demilitarized Zone (DMZ) to protect the hosts most vulnerable to attack.

41. System clocks of all information processing system within the organization or security domain shall be synchronized with an NTP Server with time zone Nepal Standard Time (GMT+5:45).

42. Licensee shall use DNSSEC in their authoritative DNS Server.

43. Licensee shall adopt best security practices for proper configurations in mail server, DHCP server etc.

44. Licensee shall comply following provisions related to log records:

(i) Store Critical System logs such as user's activity logs (e.g. log in/out time, login period, access logs, functions performed etc.) and System/Applications event and error logs.

(ii) All security related logs shall be retained for at least six months and Internet NAT logs shall be retained for at least three months or as per the directives issued by NTA.

(iii) Logged activities are reviewed and analysed on regular basis.

(iv) Logging facility and log information are well protected against tampering and unauthorized access.

Chapter-5

Provisions Relating to Application Security

45. Licensee shall adopt secure software development methodology when developing any software so that security requirements like Capability Maturity Model Integration (CMMI), Open Web Application Security Project (OWASP), Centre for Internet Security (CIS), SANS Institute, Microsoft threat modeling etc. are complied from an early stage.

46. Licensee shall use OTP (One Time Password) or other form of authentication (2-Factor Authentication and Non-Trivial Password Policy) in Mobile Based Applications (Mobile Apps) to avoid any identity theft attacks.

47. Licensee shall use applications and software which must be licensed by respective application and software providers.

48. Licensee shall use SSL (Secure Socket Layer) /TLS (Transport Layer Security) in their web applications/portals.

49. Licensee shall ensure that the applications (web/mobile applications) are thoroughly tested for security vulnerabilities before its deployments.

Chapter-6

Provisions Relating to Data Security/Privacy

50. Licensee shall apply encryption techniques for data in transit.

51. Licensee shall adopt data masking or anonymizing techniques or encryption for customer data at rest. Licensee shall use Hash/Encryption to store sensitive data.

52. Licensee shall have Non-Disclosure Agreement with employee, vendor or any other third party for prohibition of copying, reproducing, distributing or selling of licensee's digital data without the consent of licensee. The customer's digital data shall not be shared to vendor or any other third party without the consent of the customer, except in the case of Government Law Enforcement Agencies.

Chapter-7

Provisions Relating to Information System (IS) Audit

53. Licensee shall have internal security audit team for regular network / System / Critical infrastructure audit and submit the security audit report to the authority in every six (6) months.

54. Licensee shall perform penetration testing and vulnerability assessment in every three (3) months and perform required rectifications.

55. Licensee shall perform Information System (IS) audit annually to verify compliance as per the clauses of this Byelaw from NTA or the Government of Nepal designated IS Auditor(s). A security audit will require security policy and standards, audit checklists and an inventory list as indicated in **Annex-1**, which may cover different areas such as web application, network architecture, wireless communication, etc. as per this byelaw.

56. Licensee shall rectify the vulnerabilities and gaps identified by the IS Auditors in their audit reports at the soonest.

Chapter-8

Provisions Relating to Cloud Security

57. The licensee shall adopt following cloud security related measures when they are providing cloud services.

    (i) Cloud control matrix and zero trust policy (cloud) to be defined.

    (ii) Cloud Service provider should have SLA (Service Level Agreement) and NDA (non-disclosure agreement) with its client.

    (iii) IAM (Identity and Access Management) has to be used to ensure that it can be configured who is who, who is authenticated, and what devices, applications, or data they can access.

(iv) Cloud service is being audited annually by Cloud Auditor(s) designated by NTA or the Government of Nepal.

Chapter-9

Provisions Relating to CERT/Incident Response

58. Licensee shall form Incident Response team/CERT.

59. Licensee shall have its approved emergency incident response plans and measures, including communication plans, to handle incidents.

60. (i) In case of any security incidents, the licensee shall co-ordinate and work in close co-operation with the task-force of NTA, comprising the following members to minimize the loss and identify the source of attack or threat.

(1) Director, Monitoring Division of NTA ------ Coordinator

(2) Deputy Director, Frequency, QoS and Service Delivery Monitoring Section ------ Member

(3) Deputy Director, Technology Research and Development Section ------ Member

(4) Assistant Director, Technology Research and Development Section ------ Member

(5) Assistant Director, Frequency, QoS and Service Delivery Monitoring Section ------ Member Secretary

(ii) The roles, responsibility and authority of the task-force will be as defined by NTA.

(iii) The task-force can hold meetings and invite ICT security expert(s) in the meetings to discuss and resolve the security related issues.

61. (i) The above task-force shall report to a high level Steering Committee of NTA, comprising the followings, on ICT security relates issues:

(1) Chairman of NTA ------ Chairman

(2) Technical Member of NTA ------ Member

(3) ICT Security Expert, nominated by Chairman ------ Member

(4) Director, Infrastructure Division ------ Member

(5) Director, Monitoring Division ------ Member Secretary

(ii) The high level Steering Committee can hold meetings as and when necessary.

62. The above high level Steering Committee shall issue directives or provide proper guidelines to the task-force. This high level committee shall also recommend to NTA board for making policy decisions on overall ICT security related issues.

63. NTA shall develop Information Sharing Platform and Licensees shall make use of the Information Sharing Platform provided by NTA for incidents, threats and possible remedies.

Chapter- 10

Provisions Relating to Security Operations Centre (SOC)

64. Licensee shall have dedicated in-house Security Unit/Operation Centre with adequate number of security professionals.

65. All the security alerts and events must be logged and monitored 24x7 to avoid any severe impact on the service and business by Security Unit/Operation Centre.

66. Licensee shall have systems like Security Information and Event Management (SIEM) for handling of security events and logs that are generated by multiple systems.

67. The Security Unit shall take all the possible preventive measure based on security logs and events to avoid attacks.

68. Licensee shall create knowledge based database of detected threats and malware information.

Chapter-11

Provisions Relating to Cyber Security Awareness & Capacity Building

69. Licensee shall conduct security awareness programs for its employees and relevant stakeholders.

70. Licensee shall design and execute capacity building program related to cyber security to enhance employee's security skills.

71. Licensee shall make necessary arrangements to raise awareness and understanding of threats and support consumers in protecting themselves and their networks as follows:

(i) Awareness through websites/portals for practicing safe online behavior.

(ii) Collaboration with other entities/organizations for awareness and education.

(iii) Conducting workshop/seminars/training/interaction programs to educate customers/users on ICT security related mattes e.g. the importance of use of licensed software, updating and patching operating systems and applications etc.

(iv) Adopting any other methods as appropriate and necessary.

Chapter-12

Miscellaneous

72. This byelaw shall be revised regularly as per requirement.

73. In case of any disputes of the meaning of the sentence(s), or words, NTA decision will be final for interpreting the meaning.

Information System (IS) Audit Checklist

Related to byelaw no. 55 of Cyber Security Byelaw, 2020

(Illustrated below are items to be checked in a security audit in compliance and best practice perspective. This checklist may not cover all aspects, but rather acts as a preliminary reference.)

Auditor's Name: ………………………………….. Audit Date:……………

Organization Name:………………………………

Contact Details (Address, Phone):………………..

Byelaws No.	Audit Question/Description	Findings	Compliance	Remarks
Chapter-2, Provisions Relating to General Security Standards and Practices				
3.	Whether the licensee have updated recorded copy of document where all its technological assets like hardware, software, and license are managed and segregated as per criticality, usage, location, versions, owner, purchase date, update date like details.			
4.	(i) Whether there exists board approved ICT Security policies for planning, organizing, directing, controlling and monitoring of information management systems. (ii) Whether these ICT Security Policies are applied/ executed for efficient and effective management of People, Process and Technology.			
5.	Whether the Licensee has reviewed ICT Security Policies at least once a year or more frequently as per the need or as per major changes in organizational structure, infrastructure or process.			

6.	Whether the Licensee has clearly defined and updated organogram with roles and responsibilities for its personnel (system operators, system developers, network administrators, information owners, security officers, users etc.), and whether they are reviewed periodically.			
7.	Whether the Licensee has employees' related policy addressing the following items (i) Proper handling of social media, (ii) Usage of Official Devices, (iii) Usage of Personal devices and (iv) Proper handling of official emails/accounts and information.			
8.	(i) Whether the Licensee has provision for access control and proper segregation of dedicated computing environment for highly sensitive systems. (ii) Whether Access controls have been configured to ensure that users are restricted to Read, Write, Execute, Delete based on the organizational information access policy.			
9.	Whether the Licensee has promoted information security awareness throughout the organizations and arranged training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and confirm to security best practices.			
10.	Whether the Licensee has adopted risk-based approach to identify, prioritize and address the security risks and consequences associated with vulnerabilities of information systems in a consistent and effective manner and determine the mitigation measures to reduce the risks to an acceptable level.			
11.	Whether the Licensee has provisions for User Account and in general comply with the followings: (i) All user accounts and their privileges subject to an approval process and documented. (ii) Admin privileges and any other special access privileges restricted to authorized individuals and documented. (iii) Admin accounts only used to perform admin tasks and not for everyday access. (iv) Admin accounts set to require a password change in every ninety (90) days or less. (v) Every individual user has a unique user name and user account. (vi) Any user account with special privileges or admin rights removed or periodically			

	disabled when no longer required or if the individual changes role or leaves the organization or after a predefined length of inactivity e.g. if the account is not used for ninety(90) days then it is disabled.			
12.	Whether the Licensee has enforced the following rules in organization for implementing password policy: (i) Password at least ten (10) characters long. (ii) Password includes combination of upper case- and lower-case alphabets, numbers and special characters. (iii) Password not same as user name. (iv) Password not a dictionary word. (v) Password does not contain any identical characters next to each other (vi) Same Passwords not used for multiple accounts in different platforms. (vii) Passwords reused within a predetermined time period. (viii) The default password on the device changed from the default to an alternative strong password. (ix) Passwords changed after every ninety (90) days periodically. (x) Already used passwords not used while changing passwords.			
13.	(i) Whether the Licensee act proactively as a first line of defense to protect their customers from known attacks, (ii) Whether the license (i) Recommend any tools/solutions (may include Anti-virus, antispyware, anti spam, malware protection, firewall provision, advise on backup of data, identity protection etc) to protect from the possible threats via available means of communication. (ii) Detect threats/malware/botnets based on IP addresses of customers and inform them for cleaning their devices.			

14.	Whether the Licensee has used commercial licensed Operating System (OS), applications, antivirus/antimalware used in Servers, Desktop, Laptop and Mobile devices etc.			
15.	Whether the Licensee has followed the common best security practices defined by SANS, CIS etc. while using open source such as GNU General Public License, BSD license for operating system, applications, antivirus/antimalware etc.			
16.	Whether the Licensee has performed regular update of Antivirus, Database, Application Libraries, Operating System, Kernel etc.			
17.	Whether the Licensee has restricted default login for any applications, systems or software.			
18.	Whether the Licensee has locked all hardware ports (including USB, CD/DVD and External Devices) of the devices (servers) for discouraging copying files directly and use alternative methods of sharing files like file server.			
19.	Whether the Licensee has made provisions for using Centralized Authentication System like Active Directory (AD), Light Weight Directory Access Protocol (LDAP) for AAA of its employees.			
20.	Whether the Licensee has used PGP/Digital signature in email communications, documents, letters and other applications.			
21.	Whether the Licensee bind manufacturers/vendors/suppliers of hardware, software and related infrastructure to patch the vulnerabilities ensuring minimum level of security.			
22.	Whether the Licensee has used of national and international cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.			
23.	Whether the Licensee has its board approved disaster recovery and Business Continuity Policy/Procedure/Plan (BCP) to counteract interruptions to business activities and to protect critical			

	business processes from the effects of major failure or disaster: (i) Redundancy and fault tolerance shall be built into the systems to minimize the impact of attacks and data corruption. (ii) The BCP shall contain identification of attacks and security breaches, incident response plan, communication plan and escalation matrix. (iii) The BCP shall contain offsite location for backups and disaster recovery.			
24.	Whether the Licensee has established security perimeters to protect physical and IT assets. Licensee shall establish protected entry controls, such as the followings, to ensure that only authorized personnel are allowed access: (i) Badges, (ii) Limited access to buildings, (iii) Guards on entrance doors, (iv) Properly secured and tamper proof wiring, (v) Alarm doors.			

Chapter-3, Provisions Relating to Infrastructure/Network Security

25.	Whether the Licensee use DDoS Detection and Mitigation system to avoid possible DDoS attack on the network infrastructure.			
26	Whether the Licensee has implemented Flow Analyzer which shall be continuously monitored for threat intelligence (threat detection and alarming).			
27.	Whether the Licensee strictly used secure Virtual Private Network (with IPSec or SSL) when accessing the systems remotely.			
28.	Whether the Licensee map and analyze organizational communication and data flows for possible			

	security threats.			
29.	Whether the Licensee has deployed Mutually Agreed Norms for Routing Security (MANRS).			
30.	Whether the Licensee has made provisions to securely authenticate users (2 Factor Authentication/ OTP) and provide encrypted access (IPSec/SSL) to Value Added Service Provider/Third Party into the core system to avoid any security risk.			
31.	Whether the Licensee has (i) Performed Penetration testing of Critical infrastructure regularly. (ii) Identified the status of equipment by performing vulnerability assessment. (iii) Implemented standard security configuration policy on Switches & Routers. (iv) Isolated and segregated (VLAN) the networks based on needs.			
32.	Whether the Licensee routinely assess their suppliers/third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting their contractual security obligations.			
33.	Whether the Licensee has implemented Wireless Local Area Network (WLAN) security standards like WPA-2/3.			
34.	Whether the Licensee has Network Firewall and following has been implemented: (i) Firewall protecting their internal network and devices against unauthorized access. (ii) Each rule set on the firewall approved by an authorized individual and documented including an explanation of the business need of this rule. (iii) Unapproved or vulnerable services blocked at the gateway firewall. (iv) Any permissive firewall rules that are no longer required disabled as soon as possible. (v) The firewall’s boundary administration settings not accessible from the internet.			
35.	For secure Network, Whether the licensee has adopted following security measures: (i) All unnecessary user accounts, guest or admin accounts removed or disabled.			

	(ii) All network infrastructure configurations automatically backed up. (iii) All auto-run and unused features disabled. (iv) Rogue Endpoints isolated.			
36.	Whether the Licensee has implemented of minimum set of configurations for hardening network and infrastructure identified in different standards like CIS, ISO, SANS, COBIT etc.			
Chapter-4, Provisions Relating to Core System Security				
37.	Whether the Licensee has used Next Generation Firewall to protect Core Service System from any form of vulnerability and attack and shall restrict access to default login.			
38.	Whether the Licensee has frequently revisited and updated firewall policy, close unnecessary ports, define max-failed-tries-within-time-limit for saving from Brute-force attack on Remote-access ports.			
39.	Whether the Licensee has provisions for IP block listing/allow listing, Port-Knocking based on needs.			
40.	Whether the Licensee has its public facing systems and services in public Demilitarized Zone (DMZ) to protect the hosts most vulnerable to attack.			
41.	Whether the system clocks of all information processing system within the organization or security domain synchronized with an NTP Server with time zone Nepal Standard Time (GMT+5:45).			
42.	Whether the Licensee has used DNSSEC in their authoritative DNS Server.			
43.	Whether the Licensee has adopted best security practices for proper configurations in mail server, DHCP server etc.			
44.	Whether the Licensee comply following provisions related to log records: (i) Store Critical System logs such as user's activity logs (e.g. log in/out time, login period, access logs, functions performed etc.) and System/Applications event and error			

	logs. (ii) All security related logs retained for at least six months and Internet NAT logs shall be retained for at least three months or as per the directives issued by NTA. (iii) Logged activities reviewed and analysed on regular basis. (iv) Logging facility and log information well protected against tampering and unauthorized access.			
Chapter-5, Provisions Relating to Application Security				
45.	Whether the Licensee has adopted secure software development methodology when developing any software so that security requirements like Capability Maturity Model Integration (CMMI), Open Web Application Security Project (OWASP), Centre for Internet Security (CIS), SANS Institute, Microsoft threat modeling etc. and complied from an early stage.			
46.	Whether the Licensee has used OTP (One Time Password) or other form of authentication (2-Factor Authentication and Non-Trivial Password Policy) in Mobile Based Applications (Mobile Apps) to avoid any identity theft attacks.			
47.	Whether the Licensee has used applications and software which must be licensed by respective application and software providers.			
48.	Whether the Licensee has used SSL (Secure Socket Layer) /TLS (Transport Layer Security) in their web applications/portals.			
49.	Whether the web or mobile applications implemented by Licensee are thoroughly tested for security vulnerabilities.			
Chapter-6, Provisions Relating to Data Security/Privacy				
50.	Whether the Licensee apply encryption techniques for data in transit.			

51.	Whether the Licensee has adopted data masking or anonymizing techniques or encryption for customer data at rest. Licensee shall use Hash/Encryption to store sensitive data.			
52.	(i) Whether the Licensee has Non-Disclosure Agreement with employee, vendor or any other third party for prohibition of copying, reproducing, distributing or selling of licensee's digital data without the consent of licensee. (ii) The customer's digital data not shared to vendor or any other third party without the consent of the customer, except in the case of Government Law Enforcement Agencies			
Chapter-7, Provisions Relating to Information System (IS) Audit				
53.	Whether the Licensee has internal security audit team for regular network / System / Critical infrastructure audit and submit the security audit report to the authority in every six (6) months.			
54.	Whether the Licensee has performed penetration testing and vulnerability assessment in every three (3) months and performs required rectifications.			
55.	Whether the Licensee has performed Information System (IS) audit annually to verify compliance as per the clauses of this Byelaw from NTA or the Government of Nepal designated IS Auditor(s).			
56.	Whether the Licensee has rectified the vulnerabilities and gaps identified by the IS Auditors in their audit reports at the soonest.			
Chapter-8, Provisions Relating to Cloud Security				
57.	Whether the licensee has adopted following cloud security related measures when they are providing cloud services. (i) Cloud control matrix and zero trust policy (cloud) defined. (ii) Cloud Service provider have SLA (Service Level Agreement) and NDA (non-disclosure			

	agreement) with its client. (iii) IAM (Identity and Access Management) used to ensure that it can be configured who is who, who is authenticated, and what devices, applications, or data they can access. (iv) Cloud service audited annually by Cloud Auditor(s) designated by NTA or the Government of Nepal.			
Chapter-9, Provisions Relating to CERT/Incident Response				
58.	Whether the Licensee has formed Incident Response team/CERT.			
59.	Whether the Licensee has its approved emergency incident response plans and measures, including communication plans, to handle incidents.			
60.	Whether the Licensee has coordinated and worked in close cooperation with the task-force of NTA in case of security incidents to minimize the loss and identify the source of attack or threat.			
61.	Whether the licensee has sent any suggestions or advices related to ICT Security issues to NTA			
62.	Whether the Licensee has complied with the ICT Security related directives of NTA.			
63.	Whether the Licensee has used the Information Sharing Platform provided by NTA for incidents, threats and possible remedies.			

Chapter- 10, Provisions Relating to Security Operations Centre (SOC)				
64.	Whether the Licensee has dedicated in-house Security Unit/Operation Centre with adequate number of security professionals.			
65.	Whether the all the security alerts and events must be logged and monitored 24x7 to avoid any severe impact on the service and business by Security Unit/Operation Centre of the Licensee.			
66.	Whether the Licensee has systems like Security Information and Event Management (SIEM) for handling of security events and logs that are generated by multiple systems.			
67.	Whether the Security Unit of the Licensees take all the possible preventive measure based on security logs and events to avoid attacks.			
68.	Whether the Licensee has created knowledge based database of detected threats and malware information.			
Chapter-11, Provisions Relating to Cyber Security Awareness & Capacity Building				
69.	Whether the Licensee has conducted security awareness programs for its employees and relevant stakeholders.			
70.	Whether the Licensee has designed and executed capacity building program related to cyber security to enhance employee’s security skills.			
71.	Whether the Licensee has made necessary arrangements to raise awareness and understanding of threats and support consumers in protecting themselves and their networks as follows: (i) Awareness through websites/portals for practicing safe online behavior. (ii) Collaboration with other entities/organizations for awareness and education. (iii) Conducting workshop/seminars/training/interaction programs to educate customers/users on ICT security related mattes e.g. the importance of use of licensed			

	software, updating and patching operating systems and applications etc. (iv) Adopting any other methods as appropriate and necessary.			
Chapter-12, Miscellaneous				
72.	Whether the Licensee has provided any suggestions/advice to NTA to update the Cyber Security Byelaw, 2020.			
73.	Whether there has been any disputes in the meaning of the sentence(s), or words and there has been a final decision from NTA and the licensee has complied the same.			