विद्युतीय कारोवार (प्रमाणीकरण) नियमावली २०६०

विद्युतीय कारोवार अध्यादेश २०६० को दफा ७८ ले प्रदान गरेको अधिकारको प्रयोग गरी यो नियमावली बनाई लागु गरिएको छ ।

परिच्छेद १
प्रारम्भिक

१.१ यो नियमावलीको नाम "विद्युतीय कारोवार (प्रमाणीकरण) नियमावली २०६०" रहनेछ ।

१.२ यो नियमावली तुरुन्त प्रारम्भ हुनेछ ।

२. परिभाषा :

क. " अध्यादेश " भन्नाले विद्युतीय कारोवार अध्यादेश २०६० सम्झनु पर्छ ।

ख. "इजाजत" भन्नाले प्रमाणीकरण गर्ने निकायले प्रमाणीकरण गर्न पाएको इजाजतलाई जनाउनेछ ।

घ. " परीक्षक" भन्नाले अध्यादेशको दफा २७(२) बमोजिमको कार्यसम्पादन परीक्षकलाई जनाउनेछ ।

ङ " ग्राहक " भन्नाले डिजिटल हस्ताक्षर प्रमाणपत्र प्राप्त गर्न चाहने ग्राहकलाई सम्झनु पर्नेछ ।

परिच्छेद २
डिजिटल हस्ताक्षर सम्बन्धि व्यवस्था

३. डिजिटल हस्ताक्षरको सिर्जना : (Creation of Digital Signature)

कुनै विद्युतीय अभिलेख वा विद्युतीय स्वरुपमा रहेको कुनै सूचनालाई डिजिटल हस्ताक्षर गरी प्रमाणित गर्नुपर्दा हस्ताक्षर गर्नेले प्रथमतः आफूले प्रयोग गरेको सफ्टवेयरको माध्यमबाट ह्यास फंक्सन (Hash Function) प्रयोग गरी ह्यास रिजल्ट सिर्जना गर्नुपर्नेछ, जुन ह्यास रिजल्टलाई हस्ताक्षरकारीको सफटवेयरको माध्यमबाट निजको निजी साँचो प्रयोग गरी डिजिटल हस्ताक्षरको सिर्जना गर्नुपर्नेछ र यस्तो डिजिटल हस्ताक्षर कुनै विद्युतीय अभिलेख वा सूचनामा संलग्न गरी अभिलिखित गरीराख्न वा प्रेषित गर्न सकिनेछ ।

४. डिजिटल हस्ताक्षरको संपुष्टि : (Verification of Digital Signature)

डिजिटल हस्ताक्षर गरिएको कुनै विद्युतीय अभिलेख वा सूचनामा भएको डिजिटल हस्ताक्षर उत्पत्तिकर्ता भनिएको व्यक्तिको नै हो वा होइन भन्ने कुराको संपुष्टिको लागि उक्त विद्युतीय अभिलेख वा सूचनालाई सार्वजनिक साँचोको प्रयोग गरी ह्यास फंक्सनको माध्यमबाट नयाँ डिजिटल हस्ताक्षर सिर्जना गरी संपुष्टि गर्दा निम्नलिखित निष्कर्ष आएमा डिजिटल हस्ताक्षर सहि मानिनेछ :

क. यदि डिजिटल हस्ताक्षर सार्वजनिक साँचोको जोडी निजी साँचोको माध्यमबाट सिर्जना गरिएको हो,

ख. यदि सार्वजनिक साँचोको माध्यमबाट सिर्जना गरिएको ह्यास रिजल्ट मूल ह्यास रिजल्टसँग हुबहु मिल्छ जुन विद्युतीय अभिलेख डिजिटल हस्ताक्षर गर्न प्रयोग गरिएको थियो र

ग. यदि संपुष्टि गर्ने सफ्टवेयरले निम्नलिखित अवस्था ठहराई डिजिटल हस्ताक्षरको संपुष्टि गर्छ,

१. डिजिटल हस्ताक्षर गर्नेको सार्वजनिक साँचोसँग तुलना गरी सिर्जना गरेको डिजिटल हस्ताक्षरसँग मेल खाएको हुनाले उक्त हस्ताक्षर उत्पत्तिकर्ताको नै हो र

२. संपुष्टिकर्ताबाट निकालिएको ह्यास रिजल्ट र विद्युतीय अभिलेखमा संलग्न रहेको डिजिटल हस्तक्षरबाट निकालिएको ह्यास रिजल्ट समान भएको हुनाले अभिलेखमा कुनै फेरबदल गरिएको छैन,

५. स्तरहरु : (Standards)

५.१ प्रमाणीकरण गर्ने निकायले प्रयोग गर्ने सूचना प्रविधि सम्बन्धि गुणस्तर वस्तुगत र अन्तर्राष्ट्रिय मापदण्ड अनुरुपको हुनुपर्नेछ । यस्ता निकायले गर्ने निम्नलिखित कार्यहरुको सम्बन्धमा न्यूनतम स्तर **अनुसूची १** मा उल्लेख गरिए बमोजिम वा सो सरह हुनुपर्नेछ

५.२ नियन्त्रकले समयसमयमा स्तरहरु निर्धारण गरी सार्वजनिक सूचना राष्ट्रीयस्तरको दैनिक पत्रिकामा प्रकाशीत गर्नु पर्नेछ ।

५.३ नियन्त्रकले समयसमयमा निर्धारण गरिदिएको र इजाजतपत्रमा उल्लेख गरिएका अन्य गुणस्तरहरुको पालना प्रमाणीकरण गर्ने निकायले गर्नुपर्नेछ ।

५.४ डिजिटल हस्ताक्षर प्रमाणपत्रको गुणस्तर : (Standard of Digital Signature Certificate)

सबै प्रमाणीकरण गर्ने निकायहरुले जारी गरेको डिजिटल हस्ताक्षर प्रमाणपत्रहरुमा नियम ५.१ मा उल्लेख गरिएको गुणस्तरको साथै न्यूनतम रुपमा निम्नलिखित विवरणहरु समेत समावेश गरिएको हुनुपर्छ :

क. क्रमसंख्या,

ख. डिजिटल हस्ताक्षर प्रमाणपत्रको किसिम (Version of the Digital certificate)

ग. हस्ताक्षर अल्गोरिदम परिचायक (Signature Algorithm Identifier),

घ. प्रमाणीकरण गर्ने निकायको नाम,

ङ. डिजिटल हस्ताक्षरको मान्यता कायम रहने अवधि,

च. ग्राहकको नाम र
छ. ग्राहकको सार्वजनिक साँचोको विवरण

६. कुनै अभिलेख सक्कल पेश गर्नुपर्ने आवश्यकता विद्युतीय अभिलेखले पूरा गर्ने : (Original Document)

नियम ४ बमोजिम मूल स्वरुपमा परिवर्तन गरिएको छैन भनी सम्पुष्टि गरिएको अभिलेखलाई विद्युतीय स्वरुपमा सिर्जना गरिएदेखि सो अभिलेखमा कुनै पनि किसिमबाट परिवर्तन गरिएको छैन भनी विश्वास गर्न सकिने अभिलेखको रुपमा मानिनेछ ।

७. सुरक्षण कार्यविधि : (Security Procedure)

नियम ३ मा उल्लेख गरिएको प्रक्रिया बमोजिम डिजिटल हस्ताक्षर संलग्न गरिएको र नियम ४ बमोजिमको परीक्षण र सम्पुष्टिबाट हेरफेर गरिएको छैन भन्ने कुराको यकीन भएको विद्युतीय अभिलेखलाई सुरक्षित विद्युतीय अभिलेख मानिनेछ ।

८. सुरक्षित डिजिटल हस्ताक्षर : (Secured Digital Signature)

नियम ३ बमोजिम सिर्जना गरीएको र नियम ४ बमोजिम परीक्षण सम्पुष्टि गर्दा सद्दे प्रमाणित भएको डिजिटल हस्ताक्षरलाई सुरक्षित डिजिटल हस्ताक्षर मानिने छ र त्यस्तो विद्युतीय हस्ताक्षरवाला व्यक्ति नै संलग्न रहेको अभिलेख वा सूचनाको उत्पत्तिकर्ता मानिनेछ ।

९. विद्युतीय अभिलेखको प्राप्तिको भरपाई : (Acknowledgement Receipt of Electronic Record)

उत्पत्तिकर्ताले कुनै विद्युतीय अभिलेखको सम्बन्धमा त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्रापकबाट प्राप्त गरेपछि मात्र निजको हकमा त्यस्तो विद्युतीय अभिलेख बन्धनकारी हुने भनी उल्लेख नगरेको अवस्थामा त्यस्तो विद्युतीय अभिलेख प्राप्तिको सूचना वा भरपाईको सम्बन्धमा उत्पत्तिकर्ता र प्रापकबिच कुनै समय निर्धारण वा मञ्जुरी नभएको भए त्यस्तो विद्युतीय अभिलेख प्राप्त गरेको मितिले तीन दिनभित्र उत्पत्तिकर्ताले प्रापकबाट त्यस्तो विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्राप्त गरिसकेको हुनुपर्छ । यसरी प्रापकबाट विद्युतीय अभिलेख प्राप्त भएको सूचना वा भरपाई प्राप्त नभएमा त्यस्तो विद्युतीय अभिलेख उत्पत्तिकर्ताले पठाएको मानिने छैन ।

तर यस व्यवस्थाले तीन दिनको अवधि समाप्त भइ सकेपछि पनि उत्पत्तिकर्ता र प्रापक दुबैको सहमतिबाट कुनै विद्युतीय अभिलेख आदान प्रदान भएकोलाई मान्यता दिइएको अवस्थामा त्यस्तो अभिलेखको वैधानिकतालाई कुनै प्रतिकूल असर पर्ने छैन ।

१०. विद्युतीय अभिलेखको प्राप्तिको समयनिर्धारण : (Date & Time of Receipt)

उत्पत्तिकर्ता र प्रापकका विचमा अन्यथा सम्झौता भएको अवस्थामा बाहेक कुनै विद्युतीय अभिलेखको प्राप्तिको समय देहाय बमोजिम मानिनेछ :

१०.१ प्रापकको आफ्नै हक वा संचालनमा रहेको कुनै कम्प्युटरप्रणाली रहेको र सो प्रणालीको ठेगानामा प्रेषित गरिएको अभिलेखको हकमा त्यस्तो प्रणालीमा त्यस्तो अभिलेख प्राप्त भएको समय ,

१०.२ अन्य अवस्थामा प्रापकले सम्बन्धित कम्प्युटर प्रणालीबाट त्यस्तो सूचना प्राप्त गरेको समय ।

परिच्छेद ३
प्रमाणीकरण गर्ने निकाय

११. प्रमाणीकरण गर्ने निकायको इजाजतपत्र : (Licensing of Certifying Authority)

११.१ प्रमाणीकरण गर्ने निकायको रुपमा इजाजत प्राप्त गर्न चाहने फर्म वा कम्पनीले **अनुसूची २** मा उल्लेख गरिएको ढाँचामा निवेदन नियन्त्रकसमक्ष दिनुपर्नेछ ।

११.२ उपनियम ११.१ बमोजीम निवेदन प्राप्त भएपछि नियन्त्रकले आवश्यक छानविन गरी सन्तुष्ट भएमा निवेदकबाट इजाजतपत्र शुल्क वापत रु. २५,०००। पच्चीस हजार रुपयाँ लिइ अनुसूची ९ मा उल्लेख गरीए बमोजीमको ढाँचामा इजाजतपत्र जारी गर्नेछ ।

११.३ प्रमाणीकरण गर्ने निकायको रुपमा इजाजत प्राप्त गर्न चाहने फर्म वा कम्पनीले अध्यादेशको दफा १६ को उपदफा २ मा उल्लेख गरिएका कागजातहरुका अतिरिक्त निम्नलिखित कागजहरु निवेदनका साथ पेश गर्नु पर्नेछ :

क. आफुले प्रयोग गर्न चाहेको प्रमाणीकरण गर्ने प्रक्रियाको विवरण,
ख. आफ्नो दर्ताको प्रमाणपत्र,
ग. आफ्नो चुक्तापुँजी र जेथा प्रमाणित गर्न आवश्यक अन्य लिखत प्रमाणहरु,
घ. नियन्त्रकले तोकेको ढाँचामा इजाजत पाएको अवस्थामा त्यस्तो इजाजत पाएको मितिले ६ महिनाभित्र प्रमाणीकरणको काम सुरु गरी सक्नेछु भन्ने कुराको प्रत्याभूतिको रुपमा नेपाल अधिराज्यभित्रको कुनै वाणिज्य बैंकले जारी गरेको रु. २५,००,०००।०० पच्चिस लाख रुपैया बराबरको कम्तीमा छ महिना अवधिसम्म म्याद रहेको परफरमेन्स बैंक ग्यारेण्टीको प्रति र
ङ नियन्त्रकले माग गरेका अन्य विवरणहरु,

११.४ प्रमाणीकरण गर्ने निकायको रुपमा काम गर्न चाहने फर्म वा कम्पनीको निम्नलिखित योग्यता पुगेको हुनुपर्छ :

क. सो को साझेदार वा शेयरवालाको रुपमा कम्तीमा २० प्रतिशत स्वामित्व नेपाली नागरिक वा नेपाली कम्पनीको रहेको , तर नियन्त्रकले उपयुक्त ठानेको अवस्थामा कार्यसंचालन भएको मितिले एक वर्ष भित्र आवश्यक प्राविधिक जनशक्ति समेत नेपाली नै उत्पादन गरी शतप्रतिशत कामदार र कर्मचारी नेपाली प्रयोग गर्ने शर्त स्वीकार गरी प्रमाणीकरण निकायको रुपमा काम गर्न चाहने फर्म वा कम्पनीले कबुलियत गरी दिएको अवस्थामा यो बन्देजबाट छुट दिन सकिनेछ ।

ख. प्रमाणीकरण गर्ने निकायको रुपमा काम गर्नका लागि आवश्यक प्राविधिक जनशक्तिले सो फर्म वा कम्पनीले प्रमाणीकरण गर्ने निकायको रुपमा इजाजत प्राप्त गरेको अवस्थामा सो फर्म वा कम्पनीमा काम गर्न मञ्जुर गरी सम्झौता गरिदिएको र

ग. पहिलेदेखी कम्प्युटर प्रविधिसँग सम्बन्धित काममा संलग्न रहेको वा त्यस्तो कुनै काममा संलग्न रहेको विदेशी कम्पनीसँग संयुक्त लगानी गर्ने गरी सो आशयको सहमतिपत्र प्राप्त गरेको,

घ. त्यस्तो फर्म वा कम्पनीको संचालक वा कुनै शेयरवाला फौजदारी कसूरमा सजाय पाएको व्यक्ति हुनुहुनेछैन ।

११.५ कुनै प्रमाणीकरण गर्ने निकायले प्रमाणीकरण गर्ने निकायको रुपमा काम गर्ने इजाजत पाउने निर्णय भए पश्चात् अर्को वर्षको श्रावण मसान्तसम्म कायम रहने गरी रु. २५,००,०००।०० पच्चिस लाख रुपैया बराबरको बैंक ग्यारेण्टी नियन्त्रकको नाममा नियन्त्रकले तोकेको ढाँचामा नेपाल अधिराज्यभित्रको कुनै वाणिज्य बैंकबाट जारी गराई नियन्त्रकलाई बुझाउनु पर्नेछ । यस्तो बैंक ग्यारेण्टी प्रत्येक वर्ष इजाजतपत्र नवीकरण गरिएको अवस्थामा नवीकरणगराउनु पर्नेछ ।

११.६ कुनै प्रमाणीकरण गर्ने निकायले प्रमाणीकरण गर्ने निकायको रुपमा काम गर्ने इजाजत प्राप्त गरेको मितिले ६ महिनाभित्र काम सुरु गरी सक्नुपर्नेछ र यसरी काम सुरु गरे पश्चात् नियन्त्रकले नियम ११ को उपनियम (३) घ बमोजिमको बैंक ग्यारेण्टी फुकुवा गरीदिनेछ ।

११.७ कुनै प्रमाणीकरण निकायले डिजिटल हस्ताक्षर प्रमाणपत्र जारी गरे बापत प्राप्त गरेको कुल आयको २ प्रतिशत रकम मासिक रुपमा अर्को महिनाको पहिलो सप्ताहभित्र रोयल्टीको रुपमा नियन्त्रकको कार्यालयमा वा नियन्त्रकको कार्यालयले सूचित गरेको बैंक खातामा बुझाउनु पर्नेछ।

१२. प्रमाणीकरण गर्ने निकायको नवीकरण: (Renewal of Certifying Authority)

१२.१ प्रमाणीकरण गर्ने निकायले प्रत्येक वर्षको वैसाख मसान्तभित्र नविकरणको लागि **अनुसूची ३** मा उल्लेख गरिएको ढाँचामा निवेदनदिनु पर्नेछ।

१२.२ नवीकरणगर्ने निर्णय भएको मितिले ७ दिनभित्र प्रमाणीकरण गर्ने निकायले नवीकरण दस्तुर २०,०००।०० र नियम ११ को उपनियम (४) बमोजिमको बैंक ग्यारेण्टीको म्याद एक वर्ष थप गरी नियन्त्रकको कार्यालयमा बुझाउनु पर्नेछ । यस्तो नवीकरण दस्तुर इजाजतपत्र निलम्बन वा खारेज भएको अवस्थामा फिर्ता हुनेछैन ।

१२.३ नवीकरण गर्ने निर्णय पश्चात् नवीकरण दस्तुर बुझाएको र नियम ११ को उपनियम (४) बमोजिमको बैंक ग्यारेण्टी नवीकरणगरी दाखिल गरेको मितिले २ दिनभित्र नविकरणको विवरण प्रमाणपत्रमा जनाई नियन्त्रकले प्रमाणीकरण गर्ने निकायलाई प्रमाणपत्र फिर्ता दिनुपर्नेछ ।

१३. नवीकरणगर्न इन्कार गर्न सक्ने : (Refusal of Renewal)

देहायको अवस्थामा नियन्त्रकले प्रमाणीकरण गर्ने निकायको इजाजतपत्र नवीकरणगर्न इन्कार गर्नसक्नेछ, यदि :

१३.१ प्रमाणीकरण गर्ने निकायले नविकरणको दर्खास्तसाथ पेश गर्नुपर्ने कुनै लिखत, विवरण पेश गरेको छैन वा नियन्त्रकले मांग गरेको प्रमाणीकरण गर्ने निकायका साथमा वा पहुँचमा भएको कुनै लिखत वा विवरण पेश नगरेमा,

१३.२ प्रमाणीकरण गर्ने निकायको इजाजत पाएको फर्म वा कम्पनी खारेजीको प्रक्रियामा रहेको छ भन्ने कुराको विश्वासयोग्य आधार नियन्त्रकलाई प्राप्त भएमा,

१३.३ प्रमाणीकरण गर्ने निकायले आफ्नो साहुको दायित्व तिर्न नसक्ने भइ दामासही गरी पाऊँ भनी नेपाल अधिराज्यभित्रको कुनै अदालतमा फिराद दायर गरेको भएमा,

१३.४ प्रमाणीकरण गर्ने निकायले इजाजतपत्रको शर्त, नियन्त्रकले दिएको कुनै निर्देशन वा यस नियमावलीको कुनै नियमको उल्लंघन गरेको कारणले नियन्त्रकले नियम १५.५ बमोजिम बैकग्यारेण्टी जफत गरेको भएमा,

१३.५ प्रमाणीकरण गर्ने निकायको संचालक, प्रोप्राइटर, साझेदार वा कुनै अधिकृत तहको कर्मचारी निकायको कारोबारसँग सम्बन्धित कुनै विषयमा ठगी, जालसाजी वा वेइमानी गरेको ठहरेमा वा विद्युतीय कारोवार अध्यादेश अन्तर्गतको कुनै कसुरमा अभियोग प्रमाणित भएमा,

१३.६ सुरक्षा सम्बन्धि मार्गदर्शन वा आफुले पेश गरेको प्रमाणीकरण गर्ने प्रक्रिया विवरणको पालना गर्न वा गराउन प्रमाणीकरण गर्ने निकाय असफल भएमा वा त्यस्तो मार्गदर्शन वा प्रमाणीकरण गर्ने प्रक्रिया विवरणको उल्लंघन प्रमाणीकरण गर्ने निकायबाट भएमा,

१३.७ प्रमाणीकरण गर्ने निकायले नियम १९.६ बमोजिम कार्यसम्पादन परीक्षण प्रतिवेदन पेश गर्न नसकेमा वा

१३.८ कार्यसम्पादन परीक्षणबाट प्रमाणीकरण गर्ने निकायलाई त्यस्तो कार्य जारी गरिरहन दिनु उचित नदेखिएमा ,

१३.९ प्रमाणीकरण गर्ने निकायको इजाजतपत्र नवीकरणगर्न इन्कार गरेमा नियन्त्रकले सो कुराको सार्वजनिक सूचना राष्ट्रिय स्तरको दैनिक पत्रिकामा प्रकाशित गर्नुपर्नेछ ,

१४. प्रमाणीकरण गर्ने निकायको इजाजत निलम्बन गर्ने : (Suspension of License)

१४.१ अध्यादेशको दफा २० को उपदफा (१) बमोजिमको अवस्थामा नियन्त्रकले प्रमाणीकरण गर्ने निकायको इजाजत निलम्बन गर्ने आदेश दिन सक्नेछ ।

१४.२ उपनियम १४.१ बमोजिम निलम्बनको आदेश दिनुपूर्व नियन्त्रकले सम्बन्धित प्रमाणीकरण गर्ने निकायलाई आफ्नो सफाइ लिखित रुपमा प्रस्तुत गर्नका लागि ३ दिनको म्याद दिई स्पष्टिकरण सोध्नेछ ।

१४.३ सामान्यत: निलम्बनको अवधि १५ दिन बढी हुनेछैन, तर १५ दिनभित्र अध्यादेशको दफा २० (१) बमोजिमको अनुसन्धान समाप्त हुन नसकेको अवस्थामा नियन्त्रकले बढीमा १५ दिनको थप निलम्बन गर्न सक्नेछ ।

१४.४ प्रमाणीकरण गर्ने निकायको इजाजतपत्र निलम्बन गरेमा नियन्त्रकले सो कुराको सार्वजनिक सूचना राष्ट्रिय स्तरको दैनिक पत्रिकामा

प्रकाशित गर्नुपर्नेछ ,

१५.प्रमाणीकरण गर्ने निकायको इजाजत रद्द गर्ने : (Cancellation of License)

१५.१ अध्यादेशको दफा २१ को उपदफा (१) मा उल्लेख गरिएको अवस्थाको बारेमा छानविन गर्न वा दफा २६ (१) बमोजिम जाँचबुझ गर्नुपर्दा नियन्त्रकले आफूले वा आफूले अधिकार प्रत्यायोजन गरेको मातहतको कुनै कर्मचारीबाट जाँचबुझ गराउन सक्नेछ ।

१५.२ उपदफा १ बमोजिम छानविन वा जाँचबुझ गर्ने क्रममा नियन्त्रक वा निजले अधिकार प्रदान गरेको व्यक्तिले सम्बन्धित प्रमाणीकरण गर्ने निकायलाई ३ दिनको समय दिई स्पष्टीकरण सोध्न सक्नेछ ।

१५.३ छानविन वा जाँचबुझको क्रममा सबै प्रकारको सहयोग गर्ने दायित्व सम्बन्धि सम्बन्धित प्रमाणीकरण गर्ने निकायको हुनेछ ।

१५.४ छानविन वा जाँचबुझको क्रममा कुनै थप विवरण, सूचना वा जानकारी प्राप्त भएमा वा शंका उत्पन्न भएको अवस्थामा एक वा बढी पूरक स्पष्टीकरण सोध्ने अधिकार नियन्त्रक वा नियन्त्रकले अधिकार प्रदान गरेको कर्मचारीले गर्न सक्नेछ ।

१५.५ यसरी छानविन वा जाँचबुझ समाप्त भएपछि नियन्त्रकले तत्काल लागु हुने गरी वा निजले निश्चित गरेको कुनै मितिदेखि प्रभावकारी हुने गरी कुनै निर्देशन दिन वा इजाजत रद्द गर्न सक्नेछ ।

१५.६ यसरी कारवाही गर्दा प्रमाणीकरण गर्ने निकाय वा त्यसका कर्मचारीले लापर्वाही, हेलचेक्रयाई वा जानीजानी गरेको कुनै कार्य, निस्क्रियता वा दिइएको मार्गदर्शनको पालना नगरेको कारणले कसैलाई हानीनोक्सानी पुग्नगएको कुरा नियन्त्रकले जानकारी पाएमा त्यस्तो हानीनोक्सानीको लागि पछि ठहरेबमोजिम क्षतिपूर्ति उपलब्ध होस् भन्ने उद्देश्यले नियन्त्रकले आवश्यक रकम नियम ११(५) बमोजिम जारी गरिएको बैंक ग्यारेण्टी जफत गरी प्राप्त गर्न सक्नेछ ।

१५.७ प्रमाणीकरण गर्ने निकायको इजाजतपत्र रद्द गरेमा नियन्त्रकले सो कुराको सार्वजनिक सूचना राष्ट्रिय स्तरको दैनिक पत्रिकामा प्रकाशित
गर्नुपर्नेछ ।

१६. विदेशी प्रमाणीकरण गर्ने निकायलाई मान्यता दिन सक्ने : (Recognition to Foreign Certifying Authority)

१६.१ नेपाल अधिराज्य पक्ष भएको कुनै क्षेत्रिय वा अन्तर्राष्ट्रिय सन्धि वा महासन्धिले बाध्यात्मक रुपमा मान्यता दिनुपर्ने व्यवस्था गरेको अवस्थामा बाहेक नेपाल अधिराज्यभित्र मान्यता प्राप्त गर्न चाहने कुनै विदेशी प्रमाणीकरण गर्ने निकायबाट नियन्त्रकले उचित ठहराएको विवरणहरु माग गर्न सक्नेछ ।

१६.२ नियम १६.१ बमोजिम प्राप्त विवरण र अन्य आवश्यक तथ्यहरुको आधारमा नियन्त्रकले त्यस्तो विदेशी निकायलाई मान्यता दिनु उचित हुने ठहराएको अवस्थामा त्यस्तो मान्यता दिंदा त्यस्तो विदेशी निकायले नेपाल अधिराज्य भित्र कार्यालय स्थापना गर्नु पर्ने वा कुनै नेपाली साझेदार राख्नु पर्ने बाध्यात्मक शर्त राख्नुका साथै पालना गर्नुपर्ने अन्य शर्तहरु समेत तोकी पूर्वस्वीकृतिको लागि श्री ५ को सरकारसमक्ष अनुरोध गर्नेछ ।

१६.३ नियम १६.२ बमोजिम नियन्त्रकको अनुरोध प्राप्त भएको अवस्थामा श्री ५ को सरकारले आवश्यक ठह-याएमा, शर्तहरुमा परिवर्तन समेत गरी पूर्वस्वीकृति प्रदान गर्न सक्नेछ ।

१६.४ यसरी पूर्वस्वीकृति प्राप्त भएपछि नियन्त्रकले विदेशी निकायलाई मान्यता दिएको व्यहोराको सूचना नेपाल राजपत्रमा प्रकाशित गर्नुपर्नेछ ।

१६.५ मान्यता दिएको शर्तको पालना त्यस्तो विदेशी प्रमाणीकरण गर्ने निकायले नगरेको अवस्थामा वा श्री ५ को सरकारले त्यस्तो मान्यता समाप्त गर्ने निर्देशन दिएको अवस्थामा नियन्त्रकले त्यस्तो विदेशी प्रमाणीकरण गर्ने निकायको मान्यता समाप्त गर्न सक्नेछ । त्यस्तो मान्यता हटाएको सूचना नेपाल राजपत्रमा प्रकशित गर्नुपर्नेछ ।

१७. प्रमाणीकरण गर्ने निकायले काम शुरु गर्ने : (Commencement of Operation by Certifying Authority)

प्रमाणीकरण गर्ने निकायले निम्नलिखित अवस्था पश्चात् मात्र डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्ने आफ्नो व्यावसायिक कार्यसम्पादन गर्न सक्नेछ :

१७.१ प्रमाणीकरण निकायले नियन्त्रकसमक्ष पेश गरेको प्रमाणीकरण प्रक्रिया विवरणलाई नियन्त्रकले मान्यता दिएको जानकारी पाई सकेको,

१७.२ प्रमाणीकरण निकायले आफ्नो जोडी साँचो सिर्जना गरीसकेको र सो मध्ये सार्वजनिक साँचो नियन्त्रकलाई हस्तान्तरण गरीसकेको,

१७.३ प्रमाणीकरण निकायले डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्ने र व्यवस्थित गर्ने कामको लागि आवश्यक रहेको भौतिक सुविधा र संरचना नियन्त्रकले खटाएको परीक्षकले परीक्षणगरी सोलाई नियन्त्रकले उपयुक्त ठहराईसकेको र

१७.४ नेपाल अधिराज्यमा रहको अन्य प्रमाणीकरण गर्ने निकायहरुसँग पारस्परिक प्रमाणीकरणको व्यवस्था मिलाइसकेको कुराको प्रमाण नियन्त्रक समक्ष पेश गरेको ।

१८. प्रमाणीकरण गर्ने निकायले काम बन्द गर्ने : (Closure of Operation of Certifying Authority)

कुनै प्रमाणीकरण गर्ने निकायले डिजिटल हस्ताक्षर प्रमाणपत्र सम्बन्धि काम बन्द गर्न चाहेको अवस्थामा :

१८.१ सो कुराको सूचना काम बन्द गर्न चाहेको मितिले वा प्रमाणीकरण गर्ने निकायको इजाजतपत्रको म्याद समाप्त हुने मितिले कम्तीमा ९० दिन अगावै नियन्त्रकलाई दिनुपर्नेछ,

१८.२ उपदफा १ बमोजिम सूचना दिए पश्चात् कम्तीमा काम बन्द गर्न चाहेको मितिको ६० दिन अगावै सो कुराको सार्वजनिक सूचना राष्ट्रिय स्तरको दैनिक पत्रिकामा प्रकाशित गर्नुपर्नेछ ,

१८.३ आफ्ना सबै चालु रहेका ग्राहकहरुलाई र पारस्परिक डिजिटल हस्ताक्षर प्रमाणीकरको व्यवस्था मिलाइएका अन्य प्रमाणीकरण गर्ने निकायहरुलाई काम बन्द गर्ने मितिबाट कम्तीमा ६० दिन अगावै आफुले काम बन्द गर्न लागेको कुराको सूचना दिनु पर्नेछ ,

१८.४ उपदफा १, २, ३ बमोजिमका सूचनाहरु डिजिटल हस्ताक्षर सहितको इमेल वा रजिष्टर्ड पोस्टबाट पठाइनु पर्छ ।

१८.५ आफुले काम बन्द गर्ने भनी तोकेको मितिमा कुनै ग्राहकको अनुरोध भएपनि वा नभएपनि आफुले जारी गरेको सम्पुर्ण डिजिटल हस्ताक्षर प्रमाणपत्र रद्द गर्नु पर्नेछ ।

१८.६ आफुले काम बन्द गरेको बाट ग्राहकहरुलाई यथासंभव कम असुविधा होस भन्ने प्रयत्न गर्नु पर्नेछ ।

१८.७ आफुले गरेको काम कारोबार, जारी गरेको डिजिटल हस्ताक्षर प्रमाणपत्र आदी सम्बन्धि कागजात अभिलेखहरु काम बन्द गरेको मितिले ७ वर्षको अवधि सम्म नष्ट नगरी राख्नु पर्नेछ ।

१८.८ काम बन्द गर्न लागेको मिति भन्दा पछि सम्म बहाल रहने अवधि तोकिएको डिजिटल हस्ताक्षर प्रमाणपत्रका ग्राहकहरुलाई नया प्रमाणपत्र लिन लाग्ने दस्तुरमा नबढने गरी क्षतिपुर्ति दिनु पर्नेछ ।

१८.९ ग्राहकको प्रमाणपत्रको बहाल रहने अवधि समाप्त भइ सकेपछि प्रमाणीकरण गर्ने निकायले निजी साँचोलाई नष्ट गरी त्यस्तो गरेको समय र मितिको जानकारी नियन्त्रकलाई दिनुपर्नेछ ।

१९. कार्य सम्पादन परीक्षणः (Auditing)

१९.१ अध्यादेशको दफा २७ (१) को प्रयोजनको लागि दफा २७ (२) बमोजिमको योग्यता पुगेका व्यक्तिहरुलाई नियन्त्रकले सूचीकृत हुनका लागि समय समयमा सूचना निकाल्नेछ ।

१९.२ सो सूचना बमोजिम आवेदन गर्न आउने व्यक्तिहरुको योग्यताको जाँचबुझ गरी सूचीकृत गर्न सक्नेछ ।

१९.३ उपनियम १९.२ बमोजिम सूचीकृत परीक्षकहरु मध्यबाट उपयुक्त ठहराएको परीक्षकलाई प्रमाणीकरण गर्ने निकायको लागि परीक्षक नियुक्त गर्नेछ ।

१९.४ परीक्षकले प्रमाणीकरण गर्ने निकायको परीक्षणगर्दा देहाय बमोजिमको कुराहरुको समेत परीक्षण गर्नुपर्नेछ :

१९.४.१ सुरक्षा नीति र योजना,

१९.४.२ भौतिक सुरक्षा,

१९.४.३ प्रयोग भइ रहेको प्रविधिको मूल्यांकन,

१९.४.४ ग्राहकहरुसँगको सेवा व्यवस्थापन,

१९.४.५ सम्बद्ध प्रमाणीकरण अभ्यास विवरण,

१९.४.६ प्रमाणीकरण अभ्यास विवरणको पालनको स्थिति ,

१९.४.७ ग्राहक र अन्य सम्बद्ध पक्षहरुसँग भएको सम्झौता, सहमतिहरु र

१९.४.८ प्रचलित कानूनको पालना र नियन्त्रकले जारी गरेको निर्देशनहरुको पालनाको स्थिति,

१९.५ प्रमाणीकरण गर्ने निकायले देहाय बमोजिमको अवधिमा नियमीत परीक्षणहरु गराउनु पर्नेछ :

१९.५.१ अभिलेखालय (Repository) को परीक्षणप्रत्येक ३, ३ महिनामा र

१९.५.२ सुरक्षा नीति, भौतिक सुरक्षाको स्थितिर कार्यसंचालन योजना लगायतको परीक्षण प्रत्येक ६, ६ महिनामा

१९.६ प्रमाणीकरण गर्ने निकायले नियम १९ को उपनियम ५ बमोजिम परीक्षण समाप्त भएको मितिले ३० दिन भित्र त्यस्तो परीक्षण प्रतिवेदन नियन्त्रकसमक्ष दाखिल गर्नुपर्नेछ । साथै त्यस्तो परीक्षणबाट कुनै त्रुटि वा अनियमितता देखिएको अवस्थामा त्यस्तो त्रुटि वा अनियमितालाई सच्याउनको लागि आवश्यक कार्य तत्कालै प्रमाणीकरण गर्ने निकायले गर्नु पर्नेछ।

१९.७ परीक्षकको पारीश्रमिक प्रत्येक वर्ष नियन्त्रकले निर्धारण गरी सार्वजनिकरुपमा सूचना प्रकाशित गर्नेछ ।

२०. कार्यसम्पादन परीक्षक हुन नसक्ने : (Appointment of Auditor)

कुनै प्रमाणीकरण निकायको परीक्षण गर्नका लागि तोकिएको परीक्षकले देहायको अवस्थामा परीक्षण गर्नुहुदैन :

२०.१ परीक्षण गर्नुपर्ने अवधिमा वा परीक्षण सुरु गर्नुपूर्व प्रमाणीकरण निकायसँग कुनै प्रकारको स्वार्थ वा सम्बन्ध रहेको भएमा र

<u>स्पष्टीकरण</u> : यस नियमको प्रयोजनको लागि प्रमाणीकरण गर्ने निकायलाई हार्डवेयर वा सफ्टवेयर विक्री गर्ने वा कुनै प्रकारले सेवा प्रदान गर्ने कम्पनी फर्म वा व्यक्ति वा त्यस्तो कम्पनी फर्म वा व्यक्तिको कर्मचारी स्वार्थ वा सम्बन्ध रहेको व्यक्ति मानिनेछ ।

२०.२ परीक्षकको रुपमा भएको सम्बन्धबाहेक परीक्षण गर्ने निकायसँग कुनै प्रकारको आर्थिक, कानूनी र अन्य सम्बन्ध भएको वा हुने योजना रहेको।

परिच्छेद ४
डिजिटल हस्ताक्षर प्रमाणपत्र

२१. डिजिटल हस्ताक्षर प्रमाणपत्र : (Digital Signature Certificate)

२१.१ डिजिटल हस्ताक्षर प्रमाणपत्र प्राप्त गर्न चाहने पक्षले **अनुसूची ४** को ढाँचामा निवेदन दिनुपर्नेछ ।

२१.२ उपनियम २१.१ बमोजिम निवेदन दिंदा **अनुसूची ८** मा उल्लेख गरिए बमोजिम निवेदनशुल्कसमेत दाखिल गर्नुपर्नेछ ।

२१.३ उपनियम २१.१ बमोजिम दरखास्त प्राप्त भए पछी प्रमाणीकरण निकायले आवश्यक छानविन गरी सन्तुष्ट भएमा **अनुसूची ८** मा उल्लेख गरिए बमोजिमको शुल्क ग्राहकसंग लिई डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्न सक्नेछ ।

२१.४ प्रमाणीकरण गर्ने निकायले डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्दा कुनै अन्तरिम वा अस्थायी प्रमाणपत्र जारी गर्नेछैन ।

२१.५ प्रमाणीकरण गर्ने निकायले डिजिटल हस्ताक्षर प्रमाणपत्र जारी गरिपाउनका लागि वा नवीकरणका लागि आधिकारिक र कानूनसम्मत अनुरोध प्राप्त गरेको अवस्थामा मात्र त्यस्तो प्रमाणपत्र जारी गर्नेछ ।

२१.६ जारी गरिएको डिजिटल हस्ताक्षर प्रमाणपत्रमा त्यस्तो डिजिटल हस्ताक्षर अभिलिखित गरिएको एक वा बढी अभिलेखालयको सूचना रहेको हुनेछ, जसमा त्यस्तो डिजिटल हस्ताक्षर प्रमाणपत्र रद्द वा निलम्बन गरिएको अवस्थामा सो को सूचीकरण गरिएको हुनेछ ।

२१.७ प्रमाणीकरण गर्ने निकायले डिजिटल हस्ताक्षर प्रमाणपत्र जारी गरी ग्राहकले त्यसलाई स्वीकार गर्नुपूर्व त्यस्मा उल्लेख गरिएका विवरणहरु सही भएको नभएको तुलना गर्ने अवसर ग्राहकलाई दिनुपर्नेछ ।

२१.८ ग्राहकले डिजिटल हस्ताक्षर प्रमाणपत्रलाई स्वीकार गरेपछि प्रमाणीकरण गर्ने निकायले त्यस्तो डिजिटल हस्ताक्षर प्रमाणपत्र अभिलिखित गरिएको अभिलेखालयमा प्रकाशित गर्नुपर्नेछ ।

२१.९ प्रमाणीकरण गर्ने निकायले डिजिटल हस्ताक्षर प्रमाणपत्र जारी गरेपछि र ग्राहकले त्यसलाई स्वीकार गरेपछि त्यस्तो प्रमाणपत्रको बैधता र विश्वसनियतामा असर पर्नसक्ने कुनै कुराको जानकारी प्रमाणीकरण गर्ने निकायले पाएमा सो निकायले त्यस्ता कुराको सूचना तत्कालै डिजिटल हस्ताक्षर प्रमाणपत्र प्राप्त गरेको ग्राहकलाई गराउनुपर्छ ।

२१.१० डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्दा त्यस्तो प्रमाणपत्र बहाल रहने अवधि त्यसमा नै उल्लेख गरी जारी गर्नुपर्नेछ ।

२१.११ डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्नुपूर्व ग्राहक त्यस्तो प्रमाणपत्रको प्रयोग कसैको सहयोगबेगर सक्षमतापूर्वक गर्न योग्य छ भन्ने कुरामा प्रमाणीकरण निकाय विश्वस्त हुनुपर्छ ।

२२. डिजिटल हस्ताक्षर प्रमाणपत्र सिर्जना गर्ने : (Creation of Digital Signature Certificate)

प्रमाणीकरण गर्ने निकायले डिजिटल हस्ताक्षर प्रमाणपत्र सिर्जना गर्ने प्रक्रियाभित्र निम्नलिखित कुराहरु समावेश गरेको हुनुपर्छ :

२२.१ वैध र आधिकारिक रुपमा डिजिटल हस्ताक्षर प्रमाणपत्र जारी गरिपाउनका लागि निवेदन प्राप्त गर्नुपर्ने,

२२.२ नया डिजिटल हस्ताक्षर प्रमाणपत्र सिर्जना गर्ने,

२२.३ त्यस्तो प्रमाणपत्रमा जोडी साँचोसंलग्न गर्ने र

२२.४ सार्वजनिक साँचोलाई प्रयोगको लागि उपलब्ध गराउने,

२३. प्रमाणीकरण गर्ने निकायले डिजिटल हस्ताक्षर प्रमाणपत्र जारी गर्नुभन्दा पूर्व निम्नलिखित कार्य सम्पन्न गरिसकेको हुनुपर्छ :

२३.१ डिजिटल हस्ताक्षर प्रमाणपत्र प्राप्त गर्ने ग्राहक सन्देहास्पद ग्राहक (Compromised User) को सूचीमा छैन भन्ने कुरामा विश्वस्त हुनुपर्ने ,

२३.२ प्रमाणीकरण प्रक्रियाको विवरणमा उल्लेख गरिएबमोजिमको पहिचानको सत्यता परीक्षण गरिसकेको हुनुपर्ने र

२३.३ त्यस्तो डिजिटल हस्ताक्षर प्रमाणपत्रको विवरण डाइरेक्ट्रीमा प्रकाशित गर्नु हुन्छ भन्ने कुराको सहमति ग्राहकबाट लिने

२४. डिजिटल हस्ताक्षर प्रमाणपत्रको ढाँचा **अनुसूची ५** मा उल्लेख गरिए बमोजिमको हुनेछ ।

२५. डिजिटल हस्ताक्षर प्रमाणपत्रको निलम्बन : (Suspension of Digital Signature Certificate)

अध्यादेशको दफा ३२ को उपदफा (ख) बमोजिम देहाय बमोजिको सार्वजनिक हित विपरीत डिजिटल हस्ताक्षर प्रमाणपत्रको प्रयोग हुने अवस्था भएमा प्रमाणीकरण गर्ने निकायले त्यस्तो प्रमाणपत्र निलम्बन गर्न सक्नेछ :

२५.१ कुनै गैरकानूनी प्रयोजनको लागि वा गैरकानूनी उद्देश्य प्राप्तिको लागि त्यस्तो डिजिटल हस्ताक्षर प्रयोग भएको वा हुन लागेको वा हुन सक्ने अवस्था प्रमाणीकरण गर्ने निकायले देखेमा,

२५.२ ग्राहकको विरुद्ध कुनै सरकारवादी हुने फौजदारी अभियोग लागी त्यसको अनुसन्धान शुरु भएको कुराको जानकारी प्रमाणीकरण गर्ने निकायले पाएमा

२५.३ नियन्त्रकले त्यस्तो प्रमाणपत्रको प्रयोग कुनै सार्वजनिक हितविपरीतको काममा भएको वा हुन लागेको वा हुनसक्ने संभावना रहेको छ भन्ने ठानी निलम्बन गर्नका लागि प्रमाणीकरण गर्ने निकायलाई त्यस्तो प्रमाणपत्र निलम्बन गर्न निर्देशन दिएमा,

२५.४ प्रमाणीकरण गर्ने निकायले ग्राहकलाई सूचना मात्र दिई कुनै डिजिटल हस्ताक्षर प्रमाणपत्रलाई बढीमा पन्ध्र दिनसम्म निलम्बन गर्न सक्नेछ ।

२५.५ १५ दिनभन्दा बढी अवधिसम्म कुनै डिजिटल हस्ताक्षर प्रमाणपत्रलाई निलम्बन गर्नुपरेको अवस्थामा प्रमाणीकरण गर्ने निकायले ग्राहकलाई कम्तीमा ३ दिनको अवधि दिई आफ्नो लिखित सफाई पेश गर्ने मौका दिनुपर्नेछ ।

२५.६ छानविन पश्चात् त्यस्तो सार्वजनिक हित विपरीत हुने कुनै अवस्था नभएको कुरा प्रमाणीकरण गर्ने निकाय वा नियन्त्रकको निर्देशन बमोजिम निलम्बन गरिएकोमा नियन्त्रकलाई लागेमा त्यस्तो निलम्बनको आदेश रद्द हुनेछ ।

२६. डिजिटल हस्ताक्षर प्रमाणपत्र रद्द हुने : (Cancellation of Digital Signature Certificate)

२६.१ अध्यादेशको दफा ३३ को उपदफा (१) को देहायको (ख) बमोजिम देहायको अवस्थालाई सार्वजनिक हितविपरीत हुने अवस्था मानिनेछ :

२६.१.१ ग्राहकबाट कुनै गैरकानूनी प्रयोजनको लागि वा गैरकानूनी उद्देश्य प्राप्तिको लागि त्यस्तो डिजिटल हस्ताक्षर प्रयोग भएको वा हुन लागेको वा हुन सक्ने अवस्था प्रमाणीकरण गर्ने निकायले देखेमा,

२६.१.२ ग्राहकको विरुद्ध कुनै सरकारवादी हुने फौजदारी कसुरमा सजाय भोगिरहेको भएमा,

२६.१.३ नियन्त्रकले त्यस्तो प्रमाणपत्रको प्रयोग कुनै सार्वजनिक हितविपरीतको काममा भएको वा हुन लागेको वा हुन सक्ने संभावना रहेको छ भन्ने ठानी रद्द गर्न का लागि प्रमाणीकरण गर्ने निकायलाई त्यस्तो प्रमाणपत्र रद्द गर्न निर्देशन दिएमा,

२६.२ प्रमाणीकरण गर्ने निकायले डिजिटल हस्ताक्षर प्रमाणपत्र रद्द गर्नुपूर्व ग्राहक वा निजको हकवालाई लाई आफ्नो लिखित सफाइ पेश गर्नका लागि ३ दिनको अवधि दिई स्पष्टीकरण सोध्नुपर्नेछ ।

२६.३ कुनै ग्राहकको नाममा निजले उपलब्ध गराएको ठेगानामा डिजिटल हस्ताक्षरसहितको इमेल मार्फत त्यस्तो स्पष्टीकरण माग गर्न सकिनेछ ।

परिच्छेद ५
विविध

२७. विद्युतीय स्वरुपमा कागजपत्रहरु स्वीकार गर्ने : (Acceptance of Electronic Document by HMG)

२७.१ विद्युतीय स्वरुपमा कागजपत्र, दस्तुर र रकम लिन बुझ्न स्वीकार गर्ने श्री ५ को सरकारको सम्बन्धित मन्त्रालय, विभाग, कार्यालय र सरकारी स्वामित्वका संस्थानहरुले आफूले त्यस्तो कागजपत्र, दस्तुर र रकम लिन बुझ्न स्वीकार गर्ने कुराको सार्वजनिक सूचना प्रकाशित गर्नुका साथै त्यस्तो विद्युतीय कागजपत्र आदी पठाउने इमेल ठेगाना समेत सार्वजनिक गर्नुपर्नेछ।

२७.२ नियम २७.१ बमोजिम सार्वजनिक गरिएको ठेगानामा डिजिटल हस्ताक्षरसहित पठाइएको विद्युतीय स्वरुको कागजपत्र, दस्तुर र रकम आदि त्यस्तो मन्त्रालय, विभाग, कार्यालय वा संस्थानले बुझेको मानिनेछ ।

२७.३ श्री ५ को सरकारका मन्त्रालय, विभाग, कार्यालय वा सरकारी स्वामित्वका सार्वजनिक संस्थानहरुले प्रयोग गर्ने डिजिटल हस्ताक्षरको सम्बन्धमा आवश्यक प्रमाणीकरण सम्बन्धि कामको लागि प्रमाणीकरण गर्ने निकाय मध्ये कुनै एक वा बढीलाई श्री ५ को सरकारले निर्णय गरी जिम्मा दिनसक्नेछ ।

२७.४ नियम २७.३ बमोजिम जिम्मा दिनुअगाडि श्री ५ को सरकारले त्यस्तो काम गर्न इच्छुक प्रमाणीकरण गर्ने निकायहरुबाट प्रस्ताव आह्वान गरी सबैभन्दा उपयुक्त देखेको प्रस्ताव स्वीकार गर्न सक्छ ।

२८. सुरक्षा मार्गदर्शनको पालना गर्नुपर्ने : (Security Guidelines)

२८.१ प्रमाणीकरण गर्ने निकायको कार्यपद्धति तथा अभ्यास कानूनसम्मत हुनुपर्दछ ।

२८.२ प्रमाणीकरण गर्ने निकायले विद्युतीय हस्ताक्षर, सूचना तथा अन्य कुराहरुको सुरक्षा, विश्वसनीयता तथा गोप्यताको पुर्ण प्रत्याभूति हुने किसिमबाट आफ्नो कार्य सम्पादन गर्नुपर्नेछ ।

२८.३ प्रमाणीकरण गर्ने निकायले सुरक्षाको मार्गदर्शन **अनुसूची ६** र **अनूसुची** ७ मा निर्धारण गरिएबमोजिम पालना गर्नुपर्नेछ ।

२८.४ प्रमाणीकरण गर्ने निकायले प्रयोग गर्ने सूचना प्रविधि र सुरक्षा नीतिको विस्तृत विवरण तयार पार्दा नियम २८.३ मा उल्लिखित अनूसूचीमा आधारित हुनपर्ने र सो को पूर्वस्वीकृतिका लागि नियन्त्रकसमक्ष पेश गर्नुपर्नेछ ।

२९. अधिकार प्रत्यायोजन गर्न सक्ने : (Delegation of Authority)

यस नियम बमोजिम आफूलाई प्राप्त कुनै अधिकार नियन्त्रकले आफ्नो मातहतको कुनै कर्मचारीलाई प्रत्यायोजन गर्न सक्नेछ ।

३०. अंग्रेजी भाषाको प्रयोग गर्न सक्ने : (Use of English Language)

यस नियमावली बमोजिम दिनुपर्ने दर्खास्त, जारी गर्नुपर्ने, अनुमतिपत्र, प्रमाणपत्र वा आदेश निर्देशन आदिमा आवश्यकता अनुसार नियन्त्रक वा प्रमाणीकरण निकाय वा ग्राहकहरुले अंग्रेजी भाषाको प्रयोग गर्न सक्नेछन् ।

३१. अनुसूचीमा हेरफेर गर्न सक्ने : (Amendment in Annexes)

यस नियमावलीको कुनै अनुसूचीमा कुनै हेरफेर गर्नु परेको अवस्थामा नियन्त्रकले श्री ५ को सरकारको स्वीकृती लिई गर्न सक्नेछ सो कुराको सार्वजनिक सूचना राष्ट्रिय स्तरको दैनिक पत्रिकामा प्रकाशित गर्नुपर्नेछ ,

अनुसूची १

नियम ५ को उपनियम (१) सँग सम्बन्धित

प्रमाणीकरण गर्ने निकायले ओपनस्टयाण्डर्ड (Open Standard) र संसारमा प्रतिष्ठापित भएका विश्वशनीय स्तरहरु भएको सूचना प्रविधि संरचनालाई प्रयोगमा ल्याउन सक्नेछन् । विभिन्न कामहरु सम्पादन गर्नको निमित्त निम्नलिखित न्यूनतम स्तरहरु कायम हुन पर्नेछ । (The Information Technology architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important and minimum standards that may be considered for different activities associated with the Certifying Authority's functions are as below.)

Product	Standard
Public Key Infrastructure	PKIX
Digital Signature Certificates and Digital Signature revocation list	X.509. version 3 certificates as specified In ITU RFC 1422
Directory (DAP and LDAP)	X.500 for publication of certificates and Certification Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL / Structured Query Language
Public Key algorithm	DSA and RSA
Digital Hash Function Algorithm	MD5 , SHA-1 & HAVAL
Digital Encryption and Digital Signature	PKCS # 7 , ECDSA
Digital Signature Request Format	PKCS # 10
Symetric Cryptography	DES or AES
Distinguished Name	X.520

अनुसूची २

नियम ११ को उपनियम (१) सँग सम्बन्धित

प्रमाणीकरण गर्ने निकायको इजाजतपत्र प्राप्त गर्नका लागि दिइने निवेदन

श्रीमान् नियन्त्रकज्यू ,

यस संस्थाले डिजिटर हस्ताक्षर प्रमाणीकरण निकायको रुपमा काम गर्नका लागि निम्नलिखित विववरण खुलाई यो निवेदन दिएका छौं :

१. संस्था को नाम :

२. संस्थाको रजिष्टर्ड कार्यालयको ठेगाना :

३. संस्थाको को अन्य कारोवार भएका शाखा कार्यालयहरुको ठेगानाहरु :

४. संस्थाको पि इ एन नम्बर र जारी गर्ने कार्यालय :

५. संस्थाको आई एस पि को नाम :

६. संस्थाको वेवसाइटको ठेगाना :

७. संस्थाको इमेल, टेलिफोन र फयाक्स नं. :

८. संस्थाको १० प्रतिशत वा सो भन्दा बढी शेयरको स्वामित्व वा साझेदारी भएका सबैको नाम, थर, ठेगाना, :

९. संस्थाको जारी पुँजी र जम्मा जेथा :

१०. संस्थाको गत वर्षको कुल कारोवार :

११. कस्तोकस्तो डिजिटल हस्ताक्षर प्रमाणीकरण गर्न चाहेको हो :

१२. संस्थाको नेपालमा प्रमाणीकरणको काम गर्ने सुविधा भएको स्थान , ठेगाना:

१३. देहाय बमोजिमका लिखतहरु संलग्न राखेका छौं :

क. संस्थाको दर्ता प्रमाणपत्र ,
ख. संस्थाको गत वर्षको लेखापरीक्षणको प्रतिवेदन,
ग. संस्थाले प्रमाणीकरण निकायको रुपमा प्रयोग गर्न चाहेको प्रमाणीकरण गर्ने प्रक्रियाको विवरण,
घ. परफरमेन्स बैंक ग्यारेण्टी र
ङ. निवेदनपत्र दस्तुर दाखिल गरेको बैंक भौचर वा रसिद,
च. संस्थाको कामको प्रकृती अनुभवको विवरण खुलेको कम्पनीको विवरण,
छ. कम्पनीको हकमा यो निवेदनदिनका लागि संचालक समितिले गरेको निर्णयको प्रमाणित प्रतिलिपि

१४. नियम ११.४ बमोजिमको योग्यता पुगेको प्रमाणित गर्ने अन्य कागजातहरु :

यो संस्था प्रमाणीकरण निकाय नियमावली २०६० को नियम ११.४ बमोजिम योग्यता पुगेको छ र माथि उल्लेख गरिएको विवरण सत्य छ ।

निवेदक

अनुसूची ३

नियम १२ को उपनियम (१) सँग सम्बन्धित

प्रमाणीकरण गर्ने निकायको इजाजतपत्रको नवीकरण गर्नका लागि दिइने निवेदन

श्रीमान नियन्त्रक ज्यू ,

यस संस्थाले डिजिटर हस्ताक्षर प्रमाणीकरण निकायको रुपमा काम गरी आएको र आगामी आर्थिक वर्षको लागि समेत प्रमाणीकरणको काम अनवरत राख्न इच्छुक भएको हुनाले प्रमाणीकरण निकाय नियमावलीको नियम बमोजिम नवीकरण दस्तुर तिरेको भौचर । रसिद यसैसाथ राखी यो निवेदन दिन आएको छौं । अतः नवीकरणगरी पाऊँ ।

संलग्न :
सक्कल प्रमाणपत्र
नवीकरण दस्तुर तिरेको । भौचर रसीद
नवीकरण गरेको बैंक ग्यारेण्टी

निवेदक

संस्थाको नाम :
प्रमाणपत्र नं. र जारी मिति :
दस्तखत गर्नेको पद :
दस्तखत गर्नेको नाम :

अनुसूची ४

नियम २१ को उपनियम (१) सँग सम्बन्धित

डिजिटल हस्ताक्षर प्रमाणपत्र प्राप्त गर्नका लागि दिनुपर्ने निवेदन

..... (प्रमाणीकरण निकायको नाम)

.....

विषय : डिजिटल हस्ताक्षर प्रमाणपत्र जारी गरी पाऊँ ।

उपरोक्त सम्बन्धमा निवेदकले प्रामाणिक डिजिटल हस्ताक्षर प्राप्त गर्नुपर्ने भएको हुनाले निवेदन शुल्कसमेत साथै राखी यो निवेदन गरेको छु । आवश्यक विवरण र संलग्न प्रमाणहरु देहाय बमोजिमको छन् :

१. ग्राहकको नाम थर ठेगाना,

२. ग्राहकको कानूनी हैसियत ,

३. ग्राहकको पहिचान हुने प्रमाणपत्र :

३.१ प्राकृतिक व्यक्तिको हकमा नागरिकता वा राहदानी :

जारी गर्ने कार्यालय :

जारी मिति :

बहाल रहने अवधि (राहदानीको हकमा) :

३.२ कम्पनी वा सँगठित संस्था वा निकायको हकमा :

दर्ता प्रमाणपत्र वा गठन आदेश, सम्बन्धित ऐन वा राजपत्रमा जारी गरिएको सूचना :

जारी भएको मिति :

जारी गर्ने कार्यालय :

३, कुन प्रयोजनको लागि डिजिटल हस्ताक्षर प्राप्त गर्न चाहेको हो ?

क. सबै प्रकारको संभव कारोबारको लागि

ख. बैंकिङ कारोबारको लागि

ग. अन्य खरीद विक्री सम्बन्धी कारोबारको लागि

घ. कुनै लेनदेन बाहेक कुनै लिखत पत्राचार आफूले जारी गरेको भन्ने प्रमाणीकरणको लागि

४. आर्थिक कारोवारसमेत गर्न चाहेको हो भने प्रत्येक कारोबारको अधिकतम सीमा :

माथि लेखिएको बेहोरा ठिक साँचोछ, त्यस निकायलाई आवश्यक परेको अन्य विवरण र प्रमाणहरु माग भएको अवस्थामा पेश गर्नेछु ।

निवेदक

मिति :

अनुसूची ५

नियम २४ सँग सम्बन्धित
डिजिटल हस्ताक्षर प्रमाणपत्रको ढाँचा

(प्रमाणीकरण गर्ने निकायको नाम)

डिजिटल हस्ताक्षर प्रमाणपत्र

प्रमाणपत्र नं.....
क्रमसंख्या.....
....

.....लाई विद्युतीय कारोवार (प्रमाणीकरण) नियमावली २०६० को दफा २१.३ वमोजिम यस नियमावली को नीति, नियम र निर्देशनको अधिनमा रहि, १ वर्ष सम्म वहाल रहने गरि मिति २०६.. साल.....महिना.....गते, यो प्रमाणपत्र प्रदान गरिन्छ ।

सार्वजनिक साँचोको विवरण

छाप

आधिकारीक हस्ताक्षर

अनुसूची ६
नियम २८ को उपनियम (३) सँग सम्बन्धित

प्रमाणीकरण गर्ने निकायले पालना गर्नु पर्ने सुरक्षा मार्गदर्शन
Security Directives to Information Technology for Certifying Authority

जोडी साँचोको निर्माण र वितरणका साथै डिजिटल हस्ताक्षर सर्टिफिकेटको वितरण र व्यवस्थापन कार्यहरु गर्ने सबै प्रमाणीकरण गर्ने निकायले यो सुरक्षाको मार्गदर्शन अनिवार्य रुपमा पालना गर्नु पर्नेछ । यो सुरक्षा मार्गदर्शनको पालना भएमा प्रमाणीकरण गर्ने निकायले संचय गर्ने data/system/Technology र प्रदान गर्ने Services हरुको विश्वसनियमा, सुरक्षामा, उपलब्धतामा ग्राहकको विश्वास बढ्ने छ । (The security directives shall apply to all certifying authorities who perform the functions associated with creation and issue of key pairs and issue and management of digital signature certificate. These directives are aimed to protect the integrity, confidentiality, security and availability of certifying authority's services, data, and systems and gain public confidence in the technology.)

प्रमाणीकरण गर्ने निकायले आफ्ना सबै कार्यहरु सम्पादन गर्दा निम्न लिखित पक्षहरुलाई परिभाषित बनाउने, विकाश गर्ने, संचालन गर्ने परिक्षण गराउने र व्यवस्थापन गरी सुरक्षाको मापदण्ड कायम गर्नु पर्नेछ । (The certifying authority shall define, build, operate, audit and manage the followings in order to maintain the security standards in all its functions.)

1. Introduction
This document provides guidelines for the implementation and management of Information Technology Security. Due to the rapid dynamism of the security requirements, this document does not provide an exact template for the organizations to follow. However, appropriate samples of security process are provided for guidelines. It is the sole responsibility of the organizations to develop internal policies and processes that meet the guidelines set forth in this document.

The following words used in the Information Technology Security Guidelines shall be interpreted as follows:

shall: The guideline defined is a mandatory requirement, and therefore must be complied with.

should: The guideline defined is a recommended requirement. Noncompliance shall be documented and approved by the management. Where appropriate, compensating controls (further internal controls to reduce risks) shall be implemented.

must: The guideline defined is a mandatory requirement, and therefore must be complied with.

may: The guideline defined is an optional requirement. The implementation of this guideline is determined by the organization's requirement.

2. Implementation of an Information Security Programme
Successful implementation of a meaningful Information Security Programme largely rests with the support and involvement of the top management. Until and unless the senior managers of the organization understand and concur with the objectives of the information security programme its ultimate success is in question.
The Information Security Programme should be broken down into specific stages as follows:

(a) Adoption of a security policy;
(b) Security risk analysis;
(c) Development and implementation of a information classification system;
(d) Development and implementation of the security standards manual;
(e) Implementation of the management security self-assessment process;
(f) On-going security programme maintenance and enforcement; and

(g) Training.

The principal task of the security implementation is to define the responsibilities of persons within the organization. The implementation should be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him to carry out his responsibilities in this regard, proper tools, environment and supporting processes need to be established. When different pieces of information at one level are integrated to form higher value information, the responsibility for its security needs also should go up in the hierarchy to the integrator and should require higher level of authority for its access.

It should be absolutely clear with respect to each information as to who is its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. Data ownership refers to the classification of data elements and the allocation of responsibility for ensuring they are kept confidential, complete and accurate. The custodian of information is responsible for the proper implementation of security guidelines and making the information available to the users on a need to know basis.

3. Information Classification

Information assets must be classified according to their sensitivity and their importance to the organization. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundaries of the organization, it is necessary to advise them on which types of information are considered more sensitive, and how the organization would like the sensitive information handled and protected. Classification, declassification, labeling, storage, access, destruction and reproduction of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organization will result in long-term difficulties in achieving success.

Confidential is that classification of information of which unauthorized disclosure/use could cause serious damage to the organization, e.g. strategic planningdocuments.

Restricted is that classification of information of which unauthorized disclosure/use would not be in the best interest of the organization and/or its customers, e.g. computer software (programs, utilities), documentation, organization personnel data, budget information.

Internal use is that classification of information that does not require any degree of protection against disclosure within the company, e.g. operating procedures, policies and standards inter office memorandums.

Unclassified is that classification of information that requires no protection against disclosure e.g. published annual reports, periodicals.While the above classifications are appropriate for a general organization viewpoint, the following classifications may be considered:

Top Secret: It shall be applied to information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation's closest secrets and to be used with great reserve.

Secret: This shall be applied to information unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause

serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

Confidentiality: This shall be applied to information unauthorized disclosure of information which could be expected to cause damage to the security of the organization or could be prejudicial to the interest of the organization, or could affect the organization in its functioning. Most information will on proper analysis be classified no higher than confidential.

Restricted: This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.

Unclassified: This is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security

4.1 Site Design

1) The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.
2) As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.
3) Materials used for the construction of the operational site shall be fire-resistant and free of toxic chemicals.
4) Ground level windows shall be fortified with study mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.
5) Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.
6) Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified by the Fire Brigade.
7) Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.
8) Any facility that supports mission-critical and sensitive applications must be located and designed for reparability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/disaster recovery plan.

4.2 Fire Protection

Combustible materials shall not be stored within hundred meters of the operational site.

1) Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Fire Brigade or any other agency of the Government shall be installed at the operational site.
2) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.
3) Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.
4) Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted/displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.
5) There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.3 Environmental Protection

1) Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.
2) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.
3) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.
4) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.4 Physical Access

1) Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.
2) Biometric physical access security systems shall be installed to control and audit access to the operational site.
3) Physical access to the operational site at all times shall be controlled and restricted to authorized personnel only. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to restricted area within operational site.
4) Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.
5) Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorized access.
6) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.
7) Emergency exits shall be tested periodically to ensure that the access security systems are operational.
8) All opening of the Data Centre should be monitored round the clock by surveillance video cameras/CCTVs.

5. Information Management

5.1 System Administration

Each organization shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Based upon the complexity and security needs of a system or application, the System Administrator shall have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.

1) Organizations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.
2) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Security Administrator.
3) Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organization. Every instance of usage of administrator's passwords must be documented.
4) Periodic review of the access rights of all users must be performed.
5) The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorized in writing by the System Administrator (Digitally signed e-mail may be acceptable).
6) The System Administrator must take steps to safeguards classified information as prescribed by its owner.
7) The System Security Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.
8) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.
9) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.

10) The System Administrator together with the system support staff shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.
11) The System Security Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.

5.2 Sensitive Information Control

1) Information assets shall be classified and protected according to their sensitivity and criticality to the organization.
2) Procedures must be in place to handle the storage media, which has sensitive and classified information.
3) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.
4) All sensitive material shall be stamped or labeled accordingly.
5) Storage media (i.e. floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc.) containing sensitive information shall be secured according to their classification.
6) Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.
7) Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (e.g. hard disk/optical disk) and external (e.g. diskette, disk drive, tapes etc.) to the system. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

5.3 Sensitive Information Security

1) Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons.
2) Highly sensitive information shall be classified in accordance with para 3.
3) Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorization to segregated directories/files.
4) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.
5) Removable electronic storage media containing sensitive information and data must be clearly labeled and secured.
6) Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

5.4 Third Party Access

1) Access to the computer systems by other organizations shall be subjected to a similar level of security protection and controls as in these Information Technology security guidelines.
2) In case the Data Centre uses the facilities of external service/facility provider (outsourcer) for any of their operations, the use of external service/facility providers (e.g. outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by [the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.
3) The external service/facility provider (e.g. outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security Guidelines.

5.5 Prevention of Computer Misuse

1) Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.
2) Each organization shall provide adequate information to all persons, including management, systems developers and programmers, end-users, and third party users warning them against misuse of computers.
3) Effective measures to deal expeditiously with breaches of security shall be established within each organization. Such measures shall include:
    i. Prompt reporting of suspected breach;
    ii. Proper investigation and assessment of the nature of suspected breach;
    iii. Secure evidence and preserve integrity of such material as relates to the discovery of any breach;
    iv. Remedial measures.
4) All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.
5) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include:
    i. The role of the system administrator, system security administrator and management
    ii. Procedure for investigation
    iii. Areas of security review; and
    iv. Subsequent follow-up action.

6. System integrity and security measures

6.1 Use of Security Systems or Facilities

1) Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorized users from gaining entry to the information system and to prevent unauthorized access to data.
2) Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

6.2 System Access Control

1) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorize issuance of user identification (ID) and resource privileges.
2) Access to information system resources like memory, storage devices etc., sensitive utilities and data resources and programme files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.
3) The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as “administrator” or “president” or “game” etc. to protect access to the system and data resources represents a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.
4) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures governing access authorizations shall be developed, documented and implemented.
5) An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.

6) Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.
7) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorized disclosure and modification.
8) Stored passwords shall be protected by access controls from unauthorized disclosure and modification.
9) Automatic time-out for terminal inactivity should be implemented.
10) Audit trail of security-sensitive access and actions taken shall be logged.
11) All forms of audit trail shall be appropriately protected against unauthorized modification or deletion.
12) Where a second level access controls is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.
13) Activities of all remote users shall be logged and monitored closely.
14) The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g. root in UNIX, GNU administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective username to gain access to root and to re-authenticate themselves before requesting access to privileged functions.
15) The startup and shutdown procedure of the security software must be automated.
16) Sensitive Operating System files, which are more prone to hackers, must be protected against all known attacks using proven tools and techniques. That is to say no user will be able to modify them except with the permission of System Administrator.

6.3 Password Management

1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords: Minimum of eight characters without leading or trailing blanks;
    i. Shall be different from the existing password and the two previous ones;
    ii. Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and
    iii. Shall not be shared, displayed or printed.
2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.
3) Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.
4) Initial or reset passwords must be changed by the user upon first use.
5) Passwords shall always be encrypted in storage to prevent unauthorized disclosure.
6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4 Privileged User's Management

1) System privileges shall be granted to users only on a need-to-use basis.
2) Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.
3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator.

4) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.
5) Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.
6) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.5 User's Account Management

1) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following:
    i. Users shall be authorized by the computer system owner to access the computer services.
    ii. A written statement of access rights shall be given to all users.
    iii. All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.
    iv. Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgment of receipt of the accounts by the users.
    v. A formal record of all registered users of the computer services shall be maintained.
    vi. Access rights of users who have been transferred, or left the organization shall be removed immediately.
    vii. A periodic check shall be carried out for redundant user accounts and access rights that are no longer required.
    viii. Ensure that redundant user accounts are not re-issued to another user.
2) User accounts shall be suspended under the following conditions:
    i. when an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator.
    ii. immediately upon the termination of the services of an individual.
    iii. suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

6.6 Data and Resource Protection

1) All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.
2) The operating system or security system of the computer system shall:
    i. Define user authority and enforce access control to data within the computer system;
    ii. Be capable of specifying, for each named individual, a list of named data objects (e.g. file, programme) or groups of named objects, and the type of access allowed.
3) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.
4) Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.
5) Application Programmer shall not be allowed to access the production system.

7. Sensitive Systems Protection

1) Security tokens/smart cards/bio-metric technologies such as Iris recognition; finger print verification technologies etc. shall be used to complement the usage of passwords to access the computer system.
2) For computer system processing sensitive data, access by other organizations shall be prohibited or strictly controlled.
3) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

8. Data Centre Operations Security

8.1 Job Scheduling

1) Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.
2) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

8.2 System Operations Procedure

1) Procedures shall be established to ensure that only authorized and correct job stream and parameter changes are made.
2) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.
3) Procedures shall be established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment.
4) Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system.

8.3 Media Management

1) Responsibilities for media library management and protection shall be clearly defined and assigned.
2) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.
3) Access to the media library (both on-site and off-site) shall be restricted to the authorized persons only. A list of personnel authorized to enter the library shall be maintained.
4) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours.
5) A media management system shall be in place to account for all media stored on-site and off-site.
6) All incoming/outgoing media transfers shall be authorized by management and users.
7) An independent physical inventory check of all media shall be conducted at least every six months.
8) All media shall have external volume identification. Internal labels shall be fixed, where available.
9) Procedures shall be in place to ensure that only authorized addition/removal of media from the library is allowed.
10) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

8.4 Media Movement

1) Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.

2) There shall be procedures to ensure the authorized and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.
3) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

9. Data Backup and Off-site Retention

1) Back-up procedures shall be documented, scheduled and monitored.
2) Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These items include:
    i. Data files
    ii. Utilities programmes
    iii. Databases
    iv. Operating system software
    v. Applications system software
    vi. Encryption keys
    vii. Pre-printed forms
    viii. Documentation (including a copy of the business continuity plans)
3) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.
4) Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.
5) Data backup is required for all systems including personal computers, servers and distributed systems and databases.
6) Critical system data and file server software must have full backups taken weekly.
7) The backups must be kept in an area physically separate from the server.
8) If critical system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on a periodic basis to an off-site storage location.
9) Critical system data and file server software must have incremental backups taken daily.
10) Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.
11) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.
12) The business recovery plan should be prepared and tested on an annual basis.

10. Audit Trails and Verification

1) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.
2) Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, when, where, and any special information such as:
    i. Success or failure of the event
    ii. Use of authentication keys, where applicable
3) Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:
    i. Significant computer system events (e.g. configuration updates, system crashes)

ii. Security profile changes
iii. Actions taken by computer operations, system administrators, system programmers, and/or security administrators

4) The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.
5) The real time clock of the computer or communications device shall be set to Nepalese Standard Time (NST). Further there shall be a procedure that checks and corrects drift in the real time clock.
6) Computer system access records shall be kept for a minimum of two years,
7) in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behavior, shall be retained as per laws of the land.
8) Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements. in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behavior, shall be retained as per laws of the land.
9) Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.

11. Measures to Handle Computer Virus

1) Responsibilities and duties shall be assigned to ensure that all file servers and personal computers are equipped with up-to-date virus protection and detection software.
2) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.
3) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies etc. brought from outside shall be used on the data, file, PKI or computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software.
4) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of antivirus software is loaded on all data, file, PKI servers and personal computers.
5) Procedures shall be established to limit the spread of viruses to other organization information assets. Such procedures inter alia shall include:

i. Communication to other business partners and users who may be at risk from an infected resource
ii. Eradication and recovery procedures
iii. Incident report must be documented and communicated per established procedures.

6) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

12. Relocation of Hardware and Software

Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following guidelines shall apply:

i. All removable media will be removed from the computer system and kept at secure location.

ii. Internal drives will be overwritten, reformatted or removed as the situation may be.
iii. If applicable, ribbons will be removed from printers.
iv. All paper will be removed from printers.

13. Hardware and Software Maintenance

Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

1) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.
2) Maintenance of an inventory and configuration chart of hardware.
3) Identification and use of security features implemented within hardware.
4) Authorization, documentation, and control of change made to the hardware.
5) Identification of support facilities including power and air conditioning.
6) Provision of an uninterruptible power supply.
7) Maintenance of equipment and services.
8) Organization must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.
9) Organization must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.
10) Maintenance personnel will sign non-disclosure agreements.
11) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.
12) All maintenance personnel should be escorted within the operational site/ computer system and network installation room by the authorized personnel of the organization.
13) After maintenance, any exposed security parameters such as passwords, user IDs, and accounts will be changed or reset to eliminate any potential security exposures.

If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system managers or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

14. Purchase and Licensing of Hardware and Software

Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organization system or network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.

1) Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.
2) There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Copyright Act and Information Technology Security Guidelines.
3) It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.
4) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.
5) Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or

unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

15. System Software

1) All system software options and parameters shall be reviewed and approved by the management.
2) System software shall be comprehensively tested and its security functionality validated prior to implementation.
3) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.
4) Versions of system software installed on the computer system and communication devices shall be regularly updated.
5) All changes proposed in the system software must be appropriately justified and approved by an authorized party.
6) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.
7) Procedures to control changes initiated by vendors shall be in accordance with para 21 pertaining to "Change Management".
8) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.
9) System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.
10) Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

16. Documentation Security

1) All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.
2) All documentation and subsequent changes shall be reviewed and approved by an independent authorized party prior to issue.
3) Access to application software documentation and sensitive system software documentation shall be restricted to authorized personnel on a "need-to-use" basis only.
4) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.
5) Documentation shall be classified according to the sensitivity of its contents/ implications.
6) Organizations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorized access, loss of and damage to information outside normal working hours.

17. Network Communication Security

1) All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.
2) The network configuration and inventories shall be documented and maintained.
3) Prior authorization of the Network Administrator shall be obtained for making any changes to network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall

be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.

4) Physical access to communications and network sites shall be controlled and restricted to authorized individuals only in accordance with para 4.4 pertaining to "Physical Access".
5) Communication and network systems shall be controlled and restricted to authorized individuals only in accordance with para 6.2 – System Access Control.
6) As far as possible, transmission medium within the Certifying Authority's operational site should be secured against electro magnetic transmission. In this regard, use of Optical Fiber Cable and armored cable may be preferred as transmission media as the case may be.
7) Network diagnostic tools, e.g., spectrum analyzer, protocol analyzer should be used on a need basis.

18. Firewalls

1) Intelligent devices generally known as "Firewalls" shall be used to isolate organization's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorized use.
2) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organization shall be physically and logically isolated from the Internet and any other external connection by a firewall.
3) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.
4) All web servers for access by Internet users shall be isolated from other data and host servers.

19. Connectivity

1) Organization shall establish procedure for allowing connectivity of their computer network or computer system to non-organization computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.
2) All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organization's host system must adhere to the general system security and access control guidelines.
3) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organization's network.
4) As far as possible, no Internet access should be allowed to database server/ file server or server hosting sensitive data.
5) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

20. Network Administrator

1) Each organization shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.
2) Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.
3) System must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorized access, virus infection and hacking.
4) Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized.
5) Only authorized and legal software shall be used on the network.

6) Shared computer systems, network devices used for business applications shall comply with the requirement established in para 6 – System Integrity and Security Measures.

21. Change Management

21.1 Change Control

1) Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organizational responsibilities for the change management process shall be defined and assigned.
2) A risk and impact analysis, classification and prioritization process shall be established.
3) No changes to a production system shall be implemented until such changes have been formally authorized. Authorization procedures for change control shall be defined and documented.
4) Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.
5) Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.
6) Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.
7) Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody.

21.2 Testing Of Changes to Production System

1) All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parties prior to implementation.
2) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes: (i) Test objectives, (ii) A documented test plan, and (iii) acceptance criteria.

21.3 Review of Changes

1) Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorized or malicious codes.
2) Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.
3) All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.
4) Periodic management reports on the status of the changes implemented in the computer resourced in the production system shall be submitted for management review.

22. Problem Management and Reporting

1) Procedures for identifying, reporting and resolving problems, such as nonfunctioning of Certifying Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.
2) A help desk shall be set up to assist users in the resolution of problems.
3) A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources.

23. Emergency Preparedness

1) Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.
2) Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

24. Contingency Recovery Equipment and Services

1) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.
2) The business continuity plan shall be developed which inter alia include the procedures for emergency ordering of the equipment and availability of the services.
3) The need for backup hardware and other peripherals should be evaluated in accordance to business needs.

25. Security Incident Reporting and Response

1) All security related incidents must be reported to central coordinator, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organization.
2) All incidents reported, actions taken, follow-up actions, and other related information shall be documented.
3) Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

26. Disaster Recovery/Management

1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include:
    i. Emergency procedures, describing the immediate action to be taken in case of a major incident
    ii. Fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site
    iii. Restoration procedures, describing the action to be taken to return to normal operation at the original site
2) The documentation should include:
    i. definition of a disaster;
    ii. condition for activating the plan;
    iii. stages of a crisis;
    iv. who will make decisions in the crisis;
    v. role of individuals for each component of the plan;
    vi. composition of the recovery team; and
    vii. Decision making process for return to normal operation.
    viii. Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.
3) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.
4) Each component/aspect of the plan should have a person and a backup assigned to its execution.
5) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.

6) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.
7) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.

अनुसूची ७

नियम २८ को उपनियम (घ) सँग सम्बन्धित

प्रमाणीकरण गर्ने निकायको नेटवर्क सम्बन्धि सुरक्षा मार्गदर्शन

Network Security Directives to Certification Authotities

1. Introduction

This document prescribes security guidelines for the management and operation of Certifying Authorities (CAs) and is aimed at protecting the integrity, confidentiality and availability of their services, data and systems. These guidelines apply to Certifying Authorities that perform all the functions associated with generation, issue and management of Digital Signature Certificate such as:

1) Verification of registration, suspension and revocation request;
2) Generation, issuance, suspension and revocation of Digital Signature Certificates; and
3) Publication and archival of Digital Signature Certificates, suspension and revocation of information.

2. Security Management

The Certifying Authority shall define Information Technology security policies for its operation on the lines defined in Information Technology (IT) security Guidelines and Security Guidelines for Certifying Authorities. The policy shall be communicated to all personnel and widely published throughout the organization to ensure that the personnel follow the policies.

3. Physical controls – site location, construction and physical access

1) The site location, design, construction and physical security of the operational site of Certifying Authority shall be in accordance with para 4 of the Information Technology Security Guidelines
2) Physical access to the operational site housing computer servers, PKI server, communications and network devices shall be controlled and restricted to the authorized individuals only in accordance with para 4.4 of the Information Technology Security Guidelines given at Information Technology (IT) security Guidelines.
3) A Certifying Authority must:
    i. Ensure that the operational site housing PKI servers, communications and networks is protected with fire suppression system in accordance with para 4.2 of the Information Technology Security Guidelines given at Information Technology (IT) Security Guidelines.
    ii. Ensure that power and air-conditioning facilities are installed in accordance with para 4.1 of the Information Technology Security Guidelines.
    iii. Ensure that all removable media and papers containing sensitive or plain text information are listed, documented and stored in a container properly identified.
    iv. Ensure unescorted access to Certifying Authority's server is limited to those personnel identified on an access list.
    v. Ensure that the exact location of Digital Signature Certification System shall not be publicly identified.
    vi. Ensure that access security system is installed to control and audit access to the Digital Signature Certification System.
    vii. Ensure that dual control over the inventory and access cards/keys are in place.
    viii. Ensure that up-to-date list of personnel who possess the access cards/ keys is maintained at the Certifying Authority's operational site. Loss of access cards/keys shall be reported immediately to the Security Administrator; who shall take appropriate actions to prevent unauthorized access.
    ix. Ensure personnel not on the access list are properly escorted and supervised.

x. Ensure a site access log is maintained at the Certifying Authority's operational site and inspected periodically.

4) Multi-tiered access mechanism must be installed at the Certifying Authority's operational site. The facility should have clearly laid out security zones within its facility with well-defined access rights to each security zone. Each security zone must be separated from the other by floor to ceiling concrete reinforced walls. Alarm and intrusion detection system must be installed at every stage with adequate power backup capable of continuing operation even in the event of loss of main power. Electrical/Electronic circuits to external security alarm monitoring service (if used) must be supervised. No single person must have complete access to PKI Server, root keys or any computer system or network device on his/her own.
5) Entrance to the main building where the Certifying Authority's facilities such as Data Centre, PKI Server and Network devices are housed and entrance to each security zone must be video recorded round the clock. The recording should be carefully scrutinized and maintained for at least one year.
6) A Certifying Authority site must be manually or electronically monitored for unauthorized intrusion at all times in accordance with the Information Technology Security Guidelines
7) Computer System/PKI Server performing Digital Signature Certification function shall be located in a dedicated room or partition to facilitate enforcement of physical access control. The entry and exit of the said room or partition shall be automatically locked with time stamps and shall be reviewed daily by the Security Administrator.
8) Access to infrastructure components essential to operation of Certifying Authority such as power control panels, communication infrastructure, Digital Signature Certification system, cabling, etc. shall be restricted to authorized personnel.
9) By-pass or deactivation of normal physical security arrangements shall be authorized and documented by security personnel.
10) Intrusion detection systems shall be used to monitor and record physical access to the Digital Signature Certification system during and after office hours.
11) Computer System or PKI Server performing the Digital Signature Certification functions shall be dedicated to those functions and should not be used for any other purposes.
12) System software shall be verified for integrity in accordance with para 15 of the Information Technology Security Guidelines.

4. Media Storage
A Certifying Authority must ensure that storage media used by his system are protected from environment threats such as temperature, humidity and magnetic and are transported and managed

5. Waste Disposal
All media used for storage of information pertaining to all functions associated with generation, production, issue and management of Digital Signature Certificate shall be scrutinized before being destroyed or released for disposal.

6. Off-site Backup
A Certifying Authority must ensure that facility used for off-site backup, if any, shall be within the country and shall have the same level of security as the primary Certifying Authority site.

7. Change and Configuration Management
1) The components of the Certifying Authority infrastructure (e.g. cryptographic algorithm and its key parameters, operating system, system software, computer system, PKI server, firewalls, physical security, system security etc.) shall be reviewed every two years for new

technology risks and appropriate action plan shall be developed to manage the risks identified for each component.

2) The application software, system software and hardware, which are procured from questionable sources, shall not be installed and used for any function associated with generation and management of Digital Signature Certificate.
3) Software updates and patches shall be reviewed for security implications before being implemented on Certifying Authority's system.
4) Software updates and patches to rectify security vulnerability in critical systems used for Certifying Authority's operation shall be promptly reviewed and implemented.
5) Information on the software updates and patches and their implementation on Certifying Authority's system shall be clearly and properly documented.

8. Network and Communications Security

1) Certifying Authority's systems shall be protected to ensure network access control to critical systems and services from other systems in accordance with para 17, para 18, para 19 and para 20 of the Information Technology Security Guidelines
2) Network connections from the Certifying Authority's system to external networks shall be restricted to only those connections which are essential to facilitate Certifying Authority's functional processes and services. Such network connections to the external network shall be properly secured and monitored regularly.
3) Network connections should be initiated by the systems performing the functions of generation and management of Digital Signature Certificate to connect those systems performing the registration and repository functions but not vice versa. If this is not possible, compensating controls (e.g. use of proxy servers and other servers for further control) shall be implemented to protect the systems performing the function of generation and management of Digital Signature Certificate from potential attacks.
4) Systems performing the Digital Signature Certification function should be isolated to minimize their exposure to attempts to compromise the confidentiality, integrity and availability of the certification function.
5) Communication between the Certifying Authority systems connected on a network shall be secure to ensure confidentiality and integrity of the information. For example, communications between the Certifying Authority's systems connected on a network should be encrypted and digitally signed.
6) Intrusion detection tools should be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

9. System Security Audit Procedures

9.1 Types of event recorded

1) The Certifying Authority shall maintain record of all events relating to the security of his system. The records should be maintained in audit log file and shall include such events as:
   i. System start-up and shutdown;
   ii. Certifying Authority's application start-up and shutdown;
   iii. Attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;
   iv. Changes to keys of the Certifying Authority or any of his other details;
   v. Changes to Digital Signature Certificate creation policies, e.g. validity period;
   vi. Login and logoff attempts;
   vii. Unauthorized attempts at network access to the Certifying Authority's system;
   viii. Unauthorized attempts to access system files;
   ix. Generation of own keys;

x. Creation and revocation of Digital Signature Certificates;
xi. Attempts to initialize remove, enable, and disable subscribers, and
xii. update and recover their keys;
xiii. Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.

2) Monitoring and Audit Logs
   i. A Certifying Authority should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time. Records of the following application transactions shall be maintained:
      a) Registration;
      b) Certification;
      c) Publication;
      d) Suspension; and
      e) Revocation.

   ii. Records and log files shall be reviewed regularly for the following activities:
      a) Misuse;
      b) Errors;
      c) Security violations;
      d) Execution of privileged functions;
      e) Change in access control lists;
      f) Change in system configuration.

3) All logs, whether maintained through electronic or manual means, should contain the date and time of the event, and the identity of the subscriber/ subordinate/entity which caused the event.
4) A Certifying Authority should also collect and consolidate, either electronically or manually, security information which may not be generated by his system, such as:
   i. Physical access logs;
   ii. System configuration changes and maintenance;
   iii. Personnel changes;
   iv. Discrepancy and compromise reports;
   v. Records of the destruction of media containing key material, activation data, or personal subscriber information.

5) To facilitate decision-making, all agreements and correspondence relating to services provided by Certifying Authority should be collected and consolidated, either electronically or manually, at a single location.

9.2 Frequency of Audit Log Monitoring
The Certifying Authority must ensure that its audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary. Such reviews should involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews must be documented.

9.3 Retention Period for Audit Log
The Certifying Authority must retain its audit logs onsite for at least twelve months and subsequently retain them in the manner described in para 10 of the Information Technology Security Guidelines.

9.4 Protection of Audit Log
The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion. Manual audit information must be protected from unauthorized viewing, modification and destruction.

9.5 Audit Log Backup Procedures
Audit logs and audit summaries must be backed up or copied if in manual form.

9.6 Vulnerability Assessments
Events in the audit process are logged, in part, to monitor system vulnerabilities. The Certifying Authority must ensure that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

10. Records Archival

1) Digital Signature Certificates stored and generated by the Certifying Authority must be retained for at least seven years after the date of its expiration. This requirement does not include the backup of private signature keys.
2) Audit information as detailed in para 9, subscriber agreements, verification, identification and authentication information in respect of subscriber shall be retained for at least five years.
3) A second copy of all information retained or backed up must be stored at three locations within the country including the Certifying Authority site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. These secondary sites must provide adequate protection from environmental threats such as temperature, humidity and magnetism. The secondary site should be reachable in few hours.
4) All information pertaining to Certifying Authority's operation, Subscriber's application, verification, identification, authentication and Subscriber agreement shall be stored within the country. This information shall be taken out of the country only with the permission of Controller and where a properly constitutional warrant or such other legally enforceable document is produced.
5) The Certifying Authority should verify the integrity of the backups at least once every six months.
6) Information stored off-site must be periodically verified for data integrity.

11. Compromise and Disaster Recovery

11.1 Computing Resources, Software and/or Data are corrupted
The Certifying Authority must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides for business continuity procedures.

11.2 Secure facility after a natural or other type of disaster
The Certifying Authority must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

11.3 Incident Management Plan

1) An incident management plan shall be developed and approved by the management. The plan shall include the following areas:

i. Certifying Authority's certification key compromise;
ii. Hacking of systems and network;
iii. Breach of physical security;
iv. Infrastructure availability;
v. Fraudulent registration and generation of Digital Signature Certificates; and
vi. Digital Signature Certificate suspension and revocation information.

An incident response action plan shall be established to ensure the readiness of the Certifying Authority to respond to incidents. The plan should include the following areas:

i. Compromise control;
ii. Notification to user community; (if applicable)
iii. Revocation of affected Digital Signature Certificates; (if applicable)
iv. Responsibilities of personnel handling incidents;
v. Investigation of service disruption;
vi. Service restoration procedure;
vii. Monitoring and audit trail analysis; and
viii. Media and public relations.

12. Number of Persons Required Per Task
The Certifying Authority must ensure that no single individual may gain access to the Digital Signature Certificate server and the computer server maintaining all information associated with generation, issue and management of Digital Signature Certificate and private keys of the Certifying Authority. Minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any operation associated with generation, issue and management of Digital Signature Certificate and application of private key of the Certifying Authority.

13. Identification and Authentication for Each Role
All Certifying Authority personnel must have their identity and authorization verified before they are:
i. included in the access list for the Certifying Authority's site;
ii. included in the access list for physical access to the Certifying Authority's system;
iii. given a certificate for the performance of their Certifying Authority role;
iv. given an account on the PKI system.

Each of these certificates and accounts (with the exception of Certifying Authority's signing certificates) must:
i. be directly attributable to an individual; not be shared;
ii. be restricted to actions authorized for that role; and procedural controls.
iii. Certifying Authority's operations must be secured using techniques of authentication and encryption, when accessed across-a shared network.

14. Personnel Security Controls
The Certifying Authority must ensure that all personnel performing duties with respect to its operation must:
i. be appointed in writing;
ii. be bound by contract or statute to the terms and conditions of the position they are to fill;
iii. have received comprehensive training with respect to the duties they are to perform;
iv. be bound by statute or contract not to disclose sensitive Certifying Authority's security related information or subscriber information;

v. not be assigned duties that may cause a conflict of interest with their Certifying Authority's duties; and
vi. be aware and trained in the relevant aspects of the Information Technology Security Policy and Security Guidelines framed for carrying out Certifying Authority's operation.

15. Training Requirements
A Certifying Authority shall ensure that all personnel performing duties with respect to its operation must receive comprehensive training in:

i. relevant aspects of the Information Technology Security Policy and Security Guidelines framed by the Certifying Authority;
ii. all PKI software versions in use on the Certifying Authority's system;
iii. all PKI duties they are expected to perform; and
iv. disaster recovery and business continuity procedures.

16. Retraining Frequency and Requirements
The requirements of para 15 must be kept current to accommodate changes in the Certifying Authority's system. Refresher training must be conducted as and when required, and the Certifying Authority must review these requirements at least once a year.

17. Documentation Supplied to Personnel
A Certifying Authority must make available to his personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position.

18. Key Management
18.1 Generation
1) The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.
2) The key generation process shall generate statistically random key values that are resistant to known attacks.

18.2 Distribution of Keys
Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures confidentiality and integrity.

18.3 Storage
1) Certifying Authority's keys shall be stored in tamper-resistant devices and can only be activated under split-control by parties who are not involved in the set-up and maintenance of the systems and operations of the Certifying Authority. The key of the Certifying Authority may be stored in a tamper-resistant cryptographic module or split into sub-keys stored in tamper-resistant devices under the custody of the key custodians.
2) The Certifying Authority's key custodians shall ensure that the Certifying Authority's key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the Certifying Authority's management and documented.

18.4 Usage
1) A system and software integrity check shall be performed prior to Certifying Authority's key loading.

2) Custody of and access to the Certifying Authority's keys shall be under split control. In particular, Certifying Authority's key loading shall be performed under split control.

18.5 Certifying Authority's Public Key Delivery to Users
The Certifying Authority's public verification key must be delivered to the prospective Digital Signature Certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner.

19. Private Key Protection and Backup
1) The Certifying Authority must protect its private keys from disclosure.
2) The Certifying Authority must back-up its private keys. Backed-up keys must be stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.
3) The Certifying Authority's private key backups should is stored in a secure storage facility, away from where the original key is stored.

20. Method of Destroying Private Key
Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing. Private key destruction procedures must be described in the Certification Practice Statement or other publicly available document.

21. Usage Periods for the Public and Private Keys

21.1 Key Change
1) Certifying Authority and Subscriber keys shall be changed periodically.
2) Key change shall be processed as per Key Generation guidelines.
3) The Certifying Authority shall provide reasonable notice to the Subscriber's relying parties of any change to a new key pair used by the Certifying Authority to sign Digital Signature Certificates.
4) The Certifying Authority shall define its key change process that ensures reliability of the process by showing how the generation of key interlocks – such as signing a hash of the new key with the old key. All keys must have validity periods of no more than five years.

Suggested validity period:
a) Certifying Authority's root keys and associated certificates – five years;
b) Certifying Authority's private signing key - two years;
c) Subscriber Digital Signature Certificate key – three years;
d) Subscriber private key – three years.

Use of particular key lengths should be determined in accordance with departmental Threat-Risk Assessments.

21.2 Destruction
Upon termination of use of a Certifying Authority signature private key, all components of the private key and all its backup copies shall be securely destroyed.

21.3 Key Compromise
1) A procedure shall be pre-established to handle cases where a compromise of the Certifying Authority's Digital Signature private key has occurred. In such case, the Certifying Authority shall immediately revoke all affected Subscriber Digital Signature Certificates.
2) The Certifying Authority should immediately revoke the affected keys and Digital Signature Certificates in the case of Subscriber private key compromise.

3) The Certifying Authority's public keys shall be archived permanently to facilitate audit or investigation requirements.
4) Archives of Certifying Authority's public keys shall be protected from unauthorized modification.

22. Confidentiality of Subscriber's Information

1) Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the Certifying Authority's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law or a court order.
2) Data on the usage of the Digital Signature Certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the Certifying Authority in the course of its operation shall be protected to ensure the subscribers' privacy.
3) A secure communication channel between the Certifying Authority and its subscribers shall be established to ensure the authenticity, integrity and confidentiality of the exchanges (e.g. transmission of Digital Signature Certificate, password, private key) during the Digital Signature Certificate issuance process.

अनुसूची ८

नियम २१ को उपनियम (२) सँग सम्बन्धित

डिजिटल हस्ताक्षर सम्बन्धि शुल्कको दर

१. डिजिटल हस्ताक्षर पाउनको लागी दिइने निवेदन बापत शुल्क लाग्ने छैन ।
२. प्रत्येक डिजिटल हस्ताक्षर प्रमाणपत्रको न्यूनतम शुल्क रु. १००।०० (एक सय) लाग्ने छ ।

अनुसूची ९

नियम ११ को उपनियम (२) सँग सम्बन्धित
इजाजतपत्रको ढाँचा

श्री ५ को सरकार
नियन्त्रकको कार्यालय
इजाजतपत्र

इजाजतपत्र नं.....

.....लाई विद्युतीय कारोवार (प्रमाणीकरण) नियमावली २०६० को दफा ११.२ वमोजिम यस नियमावली को नीति, नियम र निर्देशनको अधिनमा रहि, ५ वर्ष सम्म वहाल रहने गरि प्रमाणीकरण गर्ने निकायको रुपमा काम गर्नको लागी मिति २०६० साल.....महिना.....गते, यो इजाजतपत्र प्रदान गरिन्छ ।

नियन्त्रक