नेपाल राष्ट्र बैंक

केन्द्रीय कार्यालय

भुक्तानी प्रणाली विभाग

अ.प्रा.निर्देशन नं.३/०७३ मितिः-२०७३/१०/१७

श्री नेपाल राष्ट्र बैंक, बैंकिङ कार्यालय लगायत उपत्यका बाहिरस्थित कार्यालय एवं यस विभागबाट भुक्तानी सम्बन्धी कार्य गर्न अनुमति लिएका इजाजतपत्रप्राप्त बैंक तथा वित्तीय संस्था, भुक्तानी प्रणाली सञ्चालक र भुक्तानी सेवा प्रदायक संस्था/संयन्त्र ।

विषयः- **विद्युतीय भुक्तानी सेवा प्रदान गर्दा अपनाउनु पर्ने सुरक्षा व्यवस्था**

महाशय,

यस बैंकबाट जारी गरिएको भुक्तानी सम्बन्धी कार्य गर्ने संस्था/संयन्त्रलाई प्रदान गरिने अनुमति नीति, २०७३ को बुँदा नं २ खण्ड (अ) १ र २ मा भएको व्यवस्था बमोजिम भुक्तानी सेवा सम्बन्धी कार्य सञ्चालन गर्दा अपनाउनु पर्ने सुरक्षा सम्बन्धमा देहाय बमोजिमका नीतिगत एवम् प्रक्रियागत व्यवस्था कायम गरिएकोले सोही बमोजिम गर्नु गराउनुहुन नेपाल राष्ट्र बैंक ऐन, २०५८ को दफा १०३ ले दिएको अधिकार प्रयोग गरी यो निर्देशन जारी गरिएको छ ।

१. भुक्तानी सम्बन्धी कार्य गर्न अनुमतिपत्रप्राप्त संस्थाले भुक्तानी कारोबारको सुरक्षा तथा सुसञ्चालनका लागि अपनाउनुपर्ने नीतिगत एवम् प्रक्रियागत व्यवस्था ।

(क) भुक्तानी कारोबारको सुरक्षा तथा जोखिम व्यवस्थापन सम्बन्धी नीतिगत एवम् प्रक्रियागत व्यवस्था पूरा गरी यस बैंकलाई जानकारी दिनुपर्नेछ । सूचनासम्बन्धी सुरक्षा र जोखिम व्यवस्थापन सम्बन्धमा कम्तीमा देहायका विषयहरु समावेश भएको हुनुपर्नेछ ।

अ) सूचनाको भौतिक तथा Environmental सुरक्षा सम्बन्धमा,

आ) हार्डवेयर तथा नेटवर्क सुरक्षा सम्बन्धमा,

इ) कम्प्युटर भाइरस तथा अन्य Malware हरुबाट सुरक्षा सम्बन्धमा,

ई) सूचनाको वर्गीकरण तथा पहुँच सम्बन्धमा,

उ) ग्राहकको सिस्टम पहुँचको Authentication सम्बन्धमा,

ऊ) Audit Trail तथा प्रणाली (System) मा भएका पहुँच (User Login) सम्बन्धमा,

ए) ग्राहकको सूचनाको गोपनीयता (Privacy) तथा गुनासो (Greivances) को व्यवस्थापन सम्बन्धमा,

ऐ) संस्थाले गरेको Outsourcing बाट हुने जोखिम व्यवस्थापन सम्बन्धमा,

ओ) साइवर सुरक्षाका सम्बन्धमा,

औ) सूचनाको सुरक्षा सम्बन्धी ग्राहक तथा अन्य सरोकारवालाहरुलाई प्रदान गर्ने सचेतना कार्यक्रम (Awareness Program) सम्बन्धमा,

अं) संस्थाभित्र हुने IT Operation को सम्बन्धमा,

अः) योजना कार्यान्वयन सम्बन्धमा ।

(ख) भुक्तानी कारोबारको सुरक्षा तथा जोखिम व्यवस्थापनका लागि प्राकृतिक तथा मानवीय क्षतिसँग सम्बन्धित सम्पूर्ण पक्ष समावेस भएको Disaster Recovery Plan (DRP) तयार गरी कार्यान्वयन गरेको हुनुपर्नेछ । DRP मा कम्तीमा देहायका विषयहरु समावेश भएको हुनुपर्नेछ ।

अ) Data Center (DC) तथा Standby Site/Disaster Recovery Site (DRS),

आ) Data, Power तथा System Back Up,

इ) Recovery Time Objective (RTO) र Recovery Point Objective (RPO) सम्बन्धमा,

ई) योजना कार्यान्वयन तथा Incident Handling सम्बन्धमा,

उ) DC र DRS मा भएको Data को Transaction तथा Data Integrity सम्बन्धमा,

ऊ) सूचनाको सुरक्षा सम्बन्धमा,

ए) योजनाको आवधिक तथा आकस्मिक परीक्षण सम्बन्धमा ।

(ग) संस्थाले सुरक्षाको प्रत्याभूतिको लागि भुक्तानी कारोबारको नियमित अनुगमन तथा आवश्यकता अनुरुप System Upgrade गरी सोको जानकारी सम्बन्धित कर्मचारी र प्रयोगकर्तालाई निरन्तर रुपमा गराउनुपर्नेछ ।

(घ) भुक्तानी प्रणाली कारोवारको System उपलब्ध गराउने संस्थाले System Upgrade गरे अनुरुप सम्बन्धित संस्थाले पनि भुक्तानी कारोबारमा आउनसक्ने सम्भावित जोखिमलाई दृष्टिगत गरी आवश्यकतानुसार आफ्नो प्रणालीको स्तरोन्नति गर्नुपर्नेछ ।

(ङ) भुक्तानी कारोबारको सुरक्षा एवं रेखदेखका लागि संस्थाले छुट्टै कर्मचारीको व्यवस्था गरेको हुनुपर्नेछ । उक्त कर्मचारीको काम, कर्तव्य, दायित्व र अधिकार स्पष्ट रुपमा तोकिएको हुनुपर्नेछ ।

२. प्रत्येक संस्थाले भुक्तानी प्रणालीको परीक्षण (System Audit) गराई प्रत्येक आर्थिक वर्ष समाप्त भएको ६ (छ) महिनाभित्र यस बैंकमा पेश गर्नुपर्नेछ । त्यस्तो परीक्षण गर्दा कम्तीमा निम्नानुसारको विषयवस्तुहरु समेटिएको हुनुपर्नेछ ।

(अ) User Authentication सम्बन्धमा,

(आ) आन्तरिक तथा वाह्य पक्षबाट प्रणालीमा पुग्न सक्ने सम्भावित जोखिम सम्बन्धमा,

(इ) सूचनाको सुरक्षा, प्रणाली (System) मा भएका Vulnerabilities,

(ई) Database and Transaction Security,

(उ) Network and Hardware Security,

(ऊ) Disaster Recovery सम्बन्धी व्यवस्था तथा कार्यान्वयनको अवस्था,

(ए) प्रणाली (System) मा प्रत्यक्ष पहुँच रोक्न सक्ने उपाय तथा आधारहरु,

(ऐ) Unauthorized Attempts का विवरणहरु,

(ओ) प्रणाली (System) मा सम्भावित जोखिम भए सो सम्बन्धी विवरणहरु ।

३. संस्थाले प्रयोग गरेका प्रणालीको पहुँचलाई व्यवस्थित गर्न आन्तरिक नियन्त्रण प्रणाली (Internal Control System) को उचित व्यवस्था गरेको हुनुपर्नेछ ।

४. कार्डमार्फत् भुक्तानी सेवा संचालन गर्ने संस्थाले Card Personalization and Dispatch, PIN Generation and Dispatch, Card तथा PIN Delivery लगायतका कार्यहरुमा उचित सुरक्षा व्यवस्था अपनाउनुपर्नेछ ।

५. भुक्तानी कारोबारलाई भरपर्दो, सुरक्षित तथा विश्वसनीय बनाउनका लागि ग्राहकले Electronic Payment Transaction Authentication गर्दा दुई तहको प्रमाणिकरण (Two Factor Authentication) सुनिश्चित हुने व्यवस्था मिलाउनुपर्नेछ । त्यस्तो सेवा सञ्चालन गर्दा उत्पन्न हुन सक्ने जोखिम र सोको न्यूनीकरण व्यवस्थापनको लागि उचित सतर्कता अपनाउनुपर्नेछ ।

६. इन्टरनेट बैंकिङमार्फत् भुक्तानी कारोबार गर्ने संस्थाले इन्टरनेट बैंकिङ सेवा आफ्ना खातावालालाई मात्र उपलब्ध गराउनुपर्नेछ ।

७. अन लाइन वा अन्य माध्यमवाट हुने Card Not Present-CNP कारोबारहरु क्रेडिट/डेविट/प्रिपेड कार्डमा नभएका अतिरिक्त सूचना प्रयोग गरी Authentication गर्नुपर्नेछ ।

भवदीय,

( )

कार्यकारी निर्देशक

बोधार्थ:

१. श्री नेपाल राष्ट्र बैंक, गभर्नरको कार्यालय ।
२. श्री नेपाल सरकार, अर्थ मन्त्रालय, वित्तीय क्षेत्र व्यवस्थापन महाशाखा, सिंहदरवार, काठमाण्डौ
३. श्री नेपाल राष्ट्र बैंक, बैंक तथा वित्तीय संस्था नियमन विभाग ।
४. श्री नेपाल राष्ट्र बैंक, बैंक सुपरिवेक्षण विभाग ।
५. श्री नेपाल राष्ट्र बैंक, विकास बैंक सुपरिवेक्षण विभाग ।
६. श्री नेपाल राष्ट्र बैंक, वित्त कम्पनी सुपरिवेक्षण विभाग ।
७. श्री नेपाल राष्ट्र बैंक, लघुवित्त प्रबर्द्धन तथा सुपरिवेक्षण विभाग ।
८. श्री नेपाल राष्ट्र बैंक, विदेशी विनिमय व्यवस्थापन विभाग
९. श्री नेपाल बैंकर्स संघ, काठमाण्डौ ।
१०. श्री नेपाल डेभलपमेन्ट बैंकर्स संघ, अनामनगर काठमाण्डौ ।
११. श्री नेपाल वित्तीय संस्था संघ, काठमाण्डौ ।
१२. श्री भुक्तानी प्रणाली सञ्चालक तथा भुक्तानी सेवा प्रदायक संस्था/संयन्त्रहरु ।