NRB IT POLICY AND GUIDELINES

वित्तीय क्षेत्रमा सूचना प्रविधिको प्रयोग उदयमान भएको छ| बैंकको कार्य प्रणाली व्यवसायिक गतिविधिको र नीति निर्माण गर्न वर्तमान समयमा सूचना प्रविधिले अहम भूमिका निर्वाह गरेको छ| बैंकिग कारोबारलाई सहज र सुरक्षित बनाउन वित्तीय संस्थाहरुलाई सूचना प्रविधि अपरिहार्य भएतापनि यसले वित्तीय संस्थाहरुमा थप cyber जोखिम निम्त्याएको छ|

सूचना प्रविधिको प्रयोगले बैंकहरुको कार्य प्रणाली, networking पूर्वधारको प्रयोग , प्रविधि वव्स्थापन साथै core बैंकिग प्रणालीमा थप cyber जोखिम थपिएको छ|

त्यसैले नेपाल राष्ट्र बैंकले सूचना प्रविधिलाई कुशल, प्रभावकारी र स्थिर रुपमा सन्चालन र नियमन गर्नका लागि NRB सूचना प्रविधि नीति र निर्देशिका २०१२ लागु गरेको छ|

Cyber जोखिम न्यूनीकरण गर्नु, बैंकहरुलाई सूचना प्रविधिको प्रयोगका लागि क्षमतावान बनाउनु, व्यापारलाई निरन्तरता दिनु, सूचनालाई सुरक्षित राख्नु र ग्राहक संगको सम्बन्ध सुधिकर्ण गर्नु NRB सूचना प्रविधि नीति र निर्देशिका २०१२को उदेश्य हो|

नेपाल राष्ट्र बैंकले जारि गरेको सूचना प्रविधि नीति र निर्देशिका २०१२मा ५ वाट उदेश्य, १२ वटा विशेषता र १० वटा निर्देशिका हरु छन|

उद्देश्य

- **सूचना प्रविधिका पुर्बधार हरु सुरक्षित, स्थिर र स्तरीय रुपमा सुनिश्चित गर्न**
- **सूचनाको उपलब्धता, अखण्डता र गोपनियतालाई सुनिश्चित गर्न,**
- **सूचना प्रविधि प्रणालीको कुशल, प्रभावकारी र आर्थिक प्रयोगको लागि प्रयोगकर्तालाई जागरूकता बढाउन**
- **सूचना प्रविधि संग सम्बन्धित जोखिम न्यूनीकरण गर्न**
- **वित्तीय क्षेत्रमा सूचना प्रणालीलाई प्रभावकारी बनाई सन्चालन गर्नका लागि सहजीकरण गर्न**

नीति

- वित्तीय सूचना प्रणाली FIS, व्यवस्थापन सूचना प्रणाली MIS, Enterprise Resource Planning जस्ता उपयुक्त IT प्रणाली लागू गरि सूचना प्रविधिलाई कुशल, प्रभावकारी र आर्थिक रुपमा सुनिश्चित गर्न।
- उचित कागजातका साथ भौतिक, सुरक्षित र संरचित सूचना प्रविधि पूर्वाधार कायम गर्न
- सूचनालाई बहुस्तरीय सुरक्षा कायम गर्न
- सूचना तथा सन्चार प्रणालीको लेखा परिक्षणलाई कार्यन्वयन गर्न
- Data हरुको सम्रक्षण गर्नका लागि नीति नियम निर्माण विकास र कार्यन्वयन गर्न
- कुशल, प्रभावकारी र आर्थिक रुपमा विपत व्यवस्थापनका लागि योजना विकास गरि सुरक्षित प्रणालीलाई असफल हुन् बाट जोगाउन र व्यारलाई निरन्तरताका लागि सहि योजना विकास गर्न
- सूचना प्रविधिका बाहिरि स्रोत तथा तेस्रो पक्ष् को संलग्नताका लागि संयन्त्र विकास र कार्यन्वयन गर्न
- सम्पूर्ण कार्यलयहरुमा सूचना प्रविधिमा एकरुपता र बैधानिकता स्थापित कायम राख्न
- नेपाल रास्ट्र बैंकमा आबद्ध वित्तीय संस्थाहरुलाई सहि सूचना प्रविधिको निर्देशन दिन्
- आईटी खरिदका लागि मापदण्डहरूको विकास गर्ने र प्राविधिक परिवर्तनहरू अनुसार समीक्षा गर्न
- नेपाल रास्ट्र बैंकका सूचना तथा प्रविधि स्रोत हरुको उचित प्रयोगका लागि आचार संहिता जारि गर्न
- कर्मचारीहरु लाई सूचना प्रविधिको प्रयोगका लागि क्षमतावान बनाउन

दिशानिर्देशहरू:

1. सूचना प्रविधिको नियमन (Information Technology- IT Governance):

- बैंकहरुको सूचना प्रविधिनीति बोर्डबाट स्वीकृत भएको र वार्षिक रुपमा पुनरावलोकन भएको हुनुपर्ने,
- बैंकले सूचना प्रविधिसंग सम्बन्धित रहेर अल्पकालीन, मध्यकालीन र दिर्घकालिन समयका लागि आवश्यक रणनीति तर्जुमा गर्ने,
- संगठनात्म संरचना अनुसार सूचना प्रविधिप्रयोगलाई व्यापक रुपमा अगाडी बढाउदै लैजाने,

- सूचना प्रविधिको कार्यनवयन र नियमनका लागि संगठनात्मक संरचना बनाउनु पर्ने व्यवस्था मिलाउने,
- बैंकलाई अन्तर्राष्ट्रिय स्तरको सूचना प्रविधिसम्बन्धि संरचना लागु गर्न प्रेरित गर्ने,
- बैंकले नयाँ प्रविधि विकास गर्नु पुर्व सूचना प्रविधिको जोखिम बृस्तीत रुपमा मूल्यांकन गर्ने,
- सूचना प्रविधिको स्रोत र साधनको प्रयोग र प्राप्तिमा संचालक समितिले ध्यान दिने,
- बैंकले सूचना प्रविधिनीतिको कार्यन्वयन गराउनको लागि सूचना सुरक्षा अधिकृतको व्यवस्था गर्ने,
- सूचना प्रविधि सम्बन्धि जोखिमलाई बैंकिग जोखिमलाई जोखिम व्यवस्थापन नीतिमा समावेश गर्ने,
- सूचना प्रविधि सम्बन्धि कार्यहरुको कार्य सम्पदान मूल्यांकन गर्ने र सोको प्रतिवेदन उच्च व्यवस्थापनमा बुझाउने,
- यस अन्तर्गत समयमा सूचना प्रविधि सम्बन्धि नियमन कार्यलाई प्रभावकारी रुपमा अगाडी बढाउने,

2. सूचना सुरक्षा (Information Security):

- बैंकले सूचना सुरक्षा नीति बनाई संचालक समितिबाट पारित गर्नुपर्ने,
- बैंकले सरोकारवालाहरुलाई सूचना प्रविधि सुरक्षा सम्बन्धि जनचेतना दिनुपर्ने,
- बैंकले प्रभावकारी सुरक्षित कम्प्युटर प्रणाली लागु गर्ने,
- सूचना सुरक्षा सम्बन्धि जोखिमको मूल्यांकन गर्ने,
- बैंकका कम्प्युटरहरुमा प्रयोग गरिने आधिकारिक र सुरक्षित हुनुपर्ने,
- सूचना प्रयोग गर्दा आउने जोखिम न्यूनीकरण गर्न आवश्यक नीति निर्माण गर्ने,
- कर्मचारीहरुमा सूचना सुरक्षा सम्बन्धि अबलम्बन गरिने नीतिहरुको पूर्ण रुपमा जानकारी गराउने,
- सूचनाको व्यकाप र रिकभरी व्यवस्था लगायतका सुरक्षा उपाय अबलम्बन गर्ने,
- यस अन्तर्गत समयमा सूचना सुरक्षा सम्बन्धि व्यवस्थापन कार्यलाई अगाडी बढाउने,

3. सूचना सुरक्षा शिक्षा (Education For Information Security) :

- सूचना सुरक्षा शिक्षा सम्बन्धि आवश्यक नीति तर्जुमा गर्ने,
- सूचना शिक्षा सम्बन्धि जनचेतनामूलक कार्यक्रम सन्चालन गर्ने,
- सूचना प्रविधिलाई सुरक्षित बनाउने जिम्मेवारी सम्बन्धित बैंकलाई हुनेछ,

- सूचना सुरक्षा सम्बन्धि शिक्षाको जानकारी सम्पूर्ण ग्राहकलाई दिनुपर्ने,
- बैंक तथा वित्तीय संस्थाले सुरक्षित बैंकिग कारोबार गर्न सक्षम छन् भन्ने कुराको निश्चित गर्नुपर्ने,
- फ्नो कार्य प्रणालीलाई सुरक्षित र सवल बनाउनु पर्ने,
- समयमा सूचना सुरक्षा शिक्षा सम्बन्धि कार्यलाई निरन्तरता दिने,

4. सूचनाको सर्वाजनिकिकरण र गुनासो व्यवस्थापन (information Disclosure and Grievance Handling):

- सूचनाको सार्वजनिकरण र गुनासो व्यवस्थापन गर्न आवश्यक नीति तर्जुमा गर्न,
- बैंकले नियमित रुपमा सूचना सम्बन्धि समस्या समाधान गर्ने प्रकिया ग्राहाकलाई जानकारी गराउने,
- बैंकहरुले सुरक्षा प्रणालीका कारण देखा परेका वा देखा पर्न सकने समस्या वा विवाद पहिचान गरि सो समाधानका लागि जानकारी प्रदान गर्ने,
- बैंकले सुरक्षा नीति र ग्राहकको गोपनियता कायम गर्ने,
- बैंकले ग्राहकलाई सेवा प्रदान गर्नुपूर्व सोको लागत बारेमा जानकारी दिनुपर्ने,
- बैंकले कारोवार समयमा उत्पन्न हुने विवादलाई कम समयमा समधान गर्ने,
- ग्राहकले अनुरोध गरेको खण्डमा बनले कारोवार सम्बन्धि गुनासो सम्बोधन गर्ने,
- बैंकले ग्राहकलाई विधुतीय कारोवार सुविधा प्रधान गर्नुपूर्व त्यसको लागत, जोखिम र लागतको बारेमा पर्याप्त जानकारी दिने,

5. सूचना प्रविधि सन्चालन (Information Technology Operation):

- सूचना प्रविधि सन्चालन सम्बन्धि आवश्यक नीति तर्जुमा गर्ने र सोको कार्यन्वयन गर्ने गराउने,
- संचालक समिति र उच्च व्यवस्थापनले सूचना प्रविधि सन्चालन सम्बन्धि कार्यलाई अनुगमन तथा मुल्यांकन गर्ने,
- सूचना प्रविधि सन्चालन सम्बन्धि कार्य विभिन्न बिभाघरुमा बिभाजन गरि सम्पादन गर्ने,
- बैंकले नयाँ-नयाँ प्रविधिलाई भित्राउने,
- बैंकले उपयुक्त डाटा माइग्रेसन नीति निर्माण गरि सुरक्षित र गोपिनिया ढंगले डाटा सर्ने,
- बैंकले समय-समयमा जोखिम निर्धारण गरि सो न्यूनीकरण गर्ने उपाय अवलम्बन गर्ने,

6. बाह्य स्रोत व्यवस्थापन (Outsourcing Management):

- बैंकले सूचना प्रविधिमा प्रयोग हुने हार्डवेयर, software तथा अन्य प्राविधिक सहायता बाह्य पक्षयबाट लिन सक्दछ,
- संचालक समिति र उच्च व्यवस्थापनले बाह्यपक्ष व्यवस्थापनको जिम्मेवारी लिनुपर्ने हुन्छ,
- बाह्य स्रोत व्यवस्थापन गर्नुपूर्व जोखिम मुल्यांकन गर्ने,
- बाह्य पक्षलाई आवश्यक मात्रामा मात्र आन्तरिक नियन्त्रन्कोपहुँच दिने,
- बाह्य व्यवस्थापन बैंकमा आउदा रास्ट्र बैंकको नियमको अधिनमा रही कार्य गर्न दिने,
- बैंकले प्रभावकारी नियन्त्रण तथा सुपरिवेक्षण प्रणाली लागु गर्ने,
- outsourcingको गोपिनियताको जिम्मेवारी बैंकले लिनुपर्ने,

7. सूचना प्रविधि परिक्षण (Information Technology-IT Audit):

- सूचना प्रविधि परिक्षण सम्बन्धि आवश्यक नीति तर्जुमा गर्ने र सोको कार्यन्वयन गर्ने गराउने,
- कार्यन्वयन गरिएका प्रविधिको प्रभावकारीताको मापन गर्ने,
- प्रविधि क्षेत्रमा आएको परिवर्तनलाई आत्मसाथ गर्नका लागि आन्तरिक तथा बाह्य बिज्ञबाट आवधिक रुपमा परिक्षण गर्ने,
- सुरक्षात्मक उपायको प्रभावकारीताको जाच गर्ने,
- यस अन्तर्गत समग्रमा सूचना प्रविधि परिक्षण कार्यलाई निरन्तरता दिने,

8. व्यवसायिक निरन्तरता एवं आकस्मिक जोखिम पुनरुत्थान योजना (Business Continuity and Disaster Recovery Planning):

- बैंकहरुको सूचना प्रविधिनीति बोर्डबाट स्वीकृत भएको र वार्षिक रुपमा पुनरावलोकन भएको हुनु पर्दछ|
- जिखिम पहिचान र व्यवस्थापन गर्न विस्तृत प्रक्रिया र दिशानिर्देश हुनु पर्दछ
- BCP लाई प्रभावकारी रुपमा कार्यन्वयन र विकास गर्नका लागि वरिष्ठ अधिकारी नियुक्त गर्नुपर्दछ

- प्रधान कार्यालय साथै सम्पूर्ण शाखा कार्यालयमा हरुमा आवश्यकता अनरुप विभिन्न विभागका वरिष्ठ अधिकारीहरू समावेश गरि BCP टोली गठन गर्नुपर्दछ
- BCP लाई प्रभावकारी रुपमा सुनिश्चित गर्न वार्षिक रुपमा पुनरावलोकन गर्नु पर्दछ,
- BCP ले सबै सम्बाभित प्राकृतिक र मानव निर्मित प्रकोप, वाह्य स्रोतको निर्भ्भरताका लागि सुरक्षित प्रणाली विकास गर्नु पर्दछ,
- बैकंले प्राकृतिक वा मानवनिर्मित विपतलाई व्यवस्थापन गर्न र क्षति भएमा पुन प्राप्तिका लागि उचित रणनीति विकास गर्नु पर्दछ,

9. सूचना प्रणाली प्राप्ति, विकास तथा कार्यन्वयन (InformationSystem Acquisition, Development and Implementation):

- सूचना प्रविधि प्राप्त गर्दा त्यसको प्राविधिक मुल्यांकन गरि सो प्रतिवेदन उच्च तहको व्यवस्थापन समक्ष पेश गर्ने,
- सूचना सुरक्षा सम्बन्धि आवश्यक software विकास प्रत्येक चरणमा गर्ने,
- बैंकले software निर्माण क्रममा हुने कमि कमजोरीलाई आवधिक रुपमा सुधार्ने,
- सूचना प्रणाली कार्यन्वयनका लागि आवश्यक नीति तर्जुमा गर्ने,
- यस अन्तर्गत समग्रमा सूचना प्रणाली प्राप्ति, विकास तथा कार्यन्वयन कार्यलाई निरन्तरता दिने,

10. जालसाजी/ ठगि व्यवस्थापन (Fraud Management):

- जालसाजी/ ठगि व्यवस्थापन गर्नका लागि आवश्यक नीति तर्जुमा गर्ने र सोको कार्यन्वयन गर्ने गराउने,
- कुनै इलेक्टोनिक शंकास्पद गतिविधि वा आक्रमण सम्बन्धमा ग्राहकलाई सचेत बनाउने,
- यस अन्तर्गत समग्रमा जालसाजी/ ठगि व्यवस्थापन गर्ने कार्यलाई निरन्तरता दिने,