# सहकारी साइवर सुरक्षा मार्गदर्शन, २०८०

**प्रस्तावना**

सहकारी अभियानको साइवर स्पेशलाई सुरक्षित बनाई संघ/संस्था एंव सदस्यहरुको सुचना, तथ्याङ्क र वित्तीय एंव बौद्धिक सम्पतिको सुरक्षा गर्न वाञ्छनीय भएकोले सहकारी साइवर सुरक्षा नीति २०८० को अधिनमा रही राष्ट्रिय सहकारी महासंघद्धारा सहकारी साइवर सुरक्षा मार्गदर्शन, २०८० तयार गरी लागु गरिएको छ ।

## १. संक्षिप्त नाम र प्रारम्भ

१. यो मार्गदर्शनको नाम "**सहकारी साइवर सुरक्षा मार्गदर्शन, २०८०**" रहेको छ । यस मार्गदशनलाई अग्रेजीमा Guideline on Cooperative Cyber Security 2023 भनिनेछ ।

२. यो मार्गदर्शन महासंघको साधारण सभाबाट स्वीकृत गरेको दिनदेखि लागु हुनेछ ।

**२. परिभाषाः**

बिषय वा प्रसंगले अर्को अर्थ नलागेमा यस मार्गदर्शनमा,

१. "उपकरण" भन्नाले सहकारी संघ/संस्थाहरुले प्रयोग गर्ने कम्प्यूटर, ल्यापटप, डिजिटल वालेट, टचावलेट, रिमुभेबल डिभाइस, डाटा केवल लगायतका विद्युतिय औजारलाई सम्झनु पर्छ ।

२. "एप्लिकेशन" भन्नाले सहकारी संघ/संस्थाले बैकिङ्ग एंव गैर बैकिङ्गक्रियाकलापमा प्रयोग गर्ने अनलाइन एवं अफलाईन प्लेटफर्मलाई सम्झनु पर्छ ।

३. "कम्प्युटर सर्भर" भन्नाले नेटवर्कमा रहेका सहभागीहरूलाई साझा सेवाहरू प्रदान गर्ने केन्द्रीय कम्प्युटर प्रणालीलाई सम्झनु पर्दछ ।

४. "रिमुभेवल डिभाइस" भन्नाले एउटा उपकरणबाट अर्को उपकरणमा डाटा सार्न प्रयोग हुने एष्ट्रर्नल हार्डडिक्स, पेन ड्राईभ, मेमोरी कार्ड लगायतलाई सम्झनु पर्दछ ।

५. "वेबसाइट" भन्नाले वेब पृष्ठहरू र सम्बन्धित सामग्रीहरूको संग्रहलाई सम्झनु पर्छ । जुन एक साझा डोमेन नामद्वारा पहिचान गरिन्छ र कम्तिमा एउटा वेब सर्भरमा प्रकाशित हुन्छ।

६. "सफ्ट्वेयर" भन्नाले कम्प्युटर चलाउन तथा सहकारी संघ/संस्थाको कारोबार, डिजाइन, इडिटिङ लगायतका विशेष कार्यहरू गर्न प्रयोग गरिने प्रोग्रामहरूको सेटलाई सम्झनु पर्छ ।

७. "संघ" भन्नाले जिल्ला, प्रदेश र विषयगत केन्द्रियस्तरका सहकारी संघलाई सम्झनुपर्छ । साथै सो शब्दले राष्ट्रिय सहकारी बैंक, विशिष्टीकृत सहकारी संघ र राष्ट्रिय सहकारी महासंघ समेतलाई जनाउनेछ ।

८. "संस्था" भन्नाले सहकारी ऐन बमोजिम गठन भएका प्रारम्भिक सहकारी संस्थाहरुलाई सम्झनु पर्छ ।

## खण्ड १

## उपकरणको प्रयोगतथा व्यवस्थापन

### ३ कम्प्युटर सर्भर व्यवस्थापन

१. मालवेयर (Malware) र रेन्समवेयर (Ransomware) जस्ता खतराहरू रोक्न पछिल्लो नविनतम सर्भर सुरक्षा सफ्टवेयरको प्रयोग गर्ने ।
२. सर्भरमा प्रयोग भएको सफ्टवेयर नियमित अद्यावधिक गर्ने ।
३. सर्भरमा सुरक्षित पासवर्डको प्रयोग गर्ने ।
४. सर्भर लगईन गर्दा तहगत सुरक्षा प्रणालीको व्यवस्था गर्ने ।
५. आगमन र बाहिर जाने नेटवर्क ट्राफिकलाई नियन्त्रण गर्न भरपर्दो फायरवालहरूको व्यवस्था गर्ने ।
६. आईटि विभाग वा सो सँग सम्बन्धित कर्मचारीलाई मात्र सर्भर एडमिन (Server Admin) लगईन गर्न अनुमति प्रदान गर्ने ।
७. सर्भरलाई साईवर हमलाबाट सुरक्षित राख्न सर्भर लगहरूको निगरानी गर्ने ।
८. साइबर आक्रमण वा प्राकृतिक प्रकोपबाट हुने क्षतिलाई कम गर्न नियमित रूपमा सर्भर डाटा ब्याकअप राख्ने ।
९. सर्भरमा भण्डारण गरिएको वा नेटवर्कमा रहेको संवेदनशील डाटालाई सुरक्षित गर्न एन्क्रिप्शन (Encryption) गर्ने ।
१०. साइबर आक्रमणको जोखिमलाई न्यूनीकरण गर्न समय समयमा जोखिम मूल्याङ्कन (Risk Assessments) गर्ने ।
११. सर्भर सुरक्षा बढाउन र डाटाहरूलाई साईवर खतराहरूबाट जोगाउन VPN (Virtual ..... Network) को प्रयोग गर्ने ।
१२. सर्भरको भएको स्थानलाई वातावरण अनुकुल वनाउने ।
१३. सर्भरको भौतिक सुरक्षाको लागि नियमित रूपमा हार्डवेयरको चेकजाँच गर्ने ।

## ४. कम्प्यूटर तथा ल्यापटपको प्रयोग

१. संघ/संस्थामा प्रयोग हुने कम्युटर र ल्यापटपमा युजर पासवर्ड राख्ने ।

२. कम्प्युटर तथा ल्यापटपमा Genuine Software को मात्र प्रयोग गर्ने ।

३. संघ/संस्थाको आवश्यकता बमोजिमका सफ्ट्वेयरहरु आइटि विभाग वा सो सँग सम्बन्धित कर्मचारी मार्फत मात्र डाउनलोड तथा स्टलको व्यवस्था गर्ने ।

४. प्रयोगमा आएका सप्टवेयर तथा वेव ब्राउजरहरु नियमित रुपमा अद्यावधिक गर्ने ।

५. Temporary File, ब्राउजिङ तथा सर्च हिष्टटीहरु ७-७ दिनमा डिलिट गर्ने ।

६. निस्क्रिय रहेका सप्टवेयरअनस्टल गर्ने तथा अनावश्यक फाइलहरु सिस्टमबाट हटाउने ।

७. आफूले प्रयोग गरेको कार्यालय उपकरण आईटि विभाग वा सम्बन्धित अधिकारीको स्वीकृत विना अन्य कसैले पनि प्रयोग गर्न नपाईने ।

८. संघ/संस्थाको नेर्टवकसँग व्यक्तिगत उपकरणहरु कनेक्ट नगराउने ।

९. संस्थागत प्रयोगमा रहेका उपकरणबाट व्यक्तिगत सामाजिक संजाल नचलाउने ।

१०. संस्थागत कार्यमा प्रयोग हुने उपकरणहरुमा इन्टरनेट सेक्युरिटी सहित एन्टिभाइरस राख्ने ।

## ५. रिमुभेवलडिभाईसको प्रयोग

१. संस्थागत कार्यका लागि छुट्टै रिमुभेवलडिभाईस प्रयोग गर्ने ।

२. संस्थागत प्रयोजनमा रहेको रिमुभेवल डिभाईस व्यक्तिगत प्रयोजनमा प्रयोग नगर्ने ।

३. अपरिचित व्यक्ति र अन्य संस्थाको अधिनमा रहेको रिमुभेवल डिभाईस संस्थागत उपकरणमा प्रयोग नगर्ने ।

४. अन्य व्यक्ति एंव संस्थाको अधिनमा रहेको रिमुभेवलडिभाईस प्रयोग गर्नुपर्ने अवस्था आएमा भाइरस स्क्यान लगायतका सुरक्षाको प्रक्रिया अवलम्बन गरेर मात्र प्रयोग गर्ने ।

## ६.वेवसाइटको प्रयोग

१. Https भएको सुरक्षित वेवसाइटमा मात्र ब्राउजिङ गर्ने ।

२. अनधिकृत वेवसाईटलाई सर्भर/फायरबाल (Firewall) मार्फत ब्लक गर्ने ।

३. वेवसाईट उत्पादक कम्पनीबाट सुरक्षाको प्रत्याभूति पश्चात दुइ पक्षिय सम्झौता भएपछि मात्रसंस्थागत वेवसाईट संचालन गर्ने ।

४. संस्थागत वेवसाइटलाई नियमित रुपमा अद्यावधिक गर्ने ।

५. संस्थागत वेवसाइटको View Page Source लाई Hide गर्ने ।

६. वेवसाइटका महत्वपूर्ण विवरणहरु नियमित रुपमा स्वतःBackup हुने व्यवस्था गर्ने ।

७. वेवसाइटमा प्रयोगमा नआएका Module तथा Features लाई (Disable) निश्कृय गर्ने ।

८. वेवसाइटमा रहेको डाटावेसमा हुने लगइन तथा सब्बक्राइभको नियमित सुपरिभिजन गर्ने ।

९. विश्वाशिलो र सुरक्षित ब्राउजरको मात्र प्रयोग गर्ने ।

१०. वेवसाइटमा उपलब्ध भएका विज्ञापन, चिट्ठा, पुरस्कार, सन्देश लगायतका लिंकहरु नखोल्ने तथा लाइक, कमेन्ट र फलो नगर्ने ।

११. अनावश्यक वेवसाइटमा लगइन नगर्ने र आवश्यक वेवसाइटमा लगइन गरेतापनि पासवर्ड सेभ नगर्ने ।

## ७. सप्टवेयर तथा एप्लिकेशनको प्रयोग

१. डेमो, क्र्याक (Crack) र पाइरेटेड सफ्टवेयर तथा एप्लिकेशनको प्रयोग नगर्ने ।

२. सप्ट्वेयर एंव एप्लिकेशनहरु डाउनलोड गर्दा व्यक्तिगत विवरण तथा क्यामेरामा पहुच मागेमा उक्त मागलाई अस्विकार गर्ने वा उक्त सप्टवेयर एंव एप्लिकेशन डाउनलोड नगर्ने ।

३. आधिकारीक एप्लिकेशनहरुमात्र संस्थागत रूपमा प्रयोग गर्ने ।

४. सप्ट्वेयर उत्पादकबाट सुरक्षाको प्रत्याभूति पश्चात दुइ पक्षिय सम्झौता भएपछि मात्र उक्त एप्लिकेशन प्रयोग गर्ने ।

## ८. उपकरणको व्यवस्थापन

१. प्रयोगमा ल्याउन नसक्ने ल्यापटप, कम्प्यूटर, पेनड्राइभ, हाडड्राइभ, मोबाइल, डाटा केबल र सप्टवेयरमा रहेका डाटाहरु पूर्ण रूपमा डिलिट गरेपछि मात्र उक्त उपकरणहरूलाई नष्ट (Dispose) गर्ने ।

२. संस्थागत प्रयोजनमा रहेका विद्युतिय कार्डहरुको प्रयोजन समाप्त भएपश्चात कार्डमा रहेको Chips/Barcode लाई उक्त कार्डबाट अलग गराई नष्ट (Dispose) गर्ने ।

# खण्ड २
# पासवर्डको प्रयोग तथा व्यवस्थापन

## ९. पासवर्डको प्रयोग तथा व्यवस्थापन

१. पासवर्ड कम्तिमा ८ वटा अक्षरको राख्ने ।

२. पासवर्ड राख्दा ठूलो अक्षर, सानो अक्षर, अङ्क, सिम्बोलहरु(Special Characters)को प्रयोग गर्ने ।

३. संघ/संस्थाको स्थापना मिति, स्थान वा प्रयोग गर्ने व्यक्तिको नाम, जन्ममिति, जन्मस्थान र मोबाइल नम्बर पासवर्डको रुपमा नराख्ने ।

४. प्रचलित एंव प्रसिद्ध नाम तथा स्थानहरु पासवर्डको रुपमा नराख्ने ।

५. वेवसाईटमा रहेको Application Account मा पासवर्ड सेभ नगर्ने ।

६. फरक फरक खाता(Application Accounts)को लागि फरक फरक पासवर्ड राख्ने ।

७. वढिमा ३-३ महिनामा पासवर्ड परिवर्तन गर्ने ।

८. एक पटक प्रयोगमा आइसकेको पासवर्ड सोही खातामा पूनः प्रयोग नगर्ने । साथै सोहि पासवर्ड अन्य खातामा समेत प्रयोग नगर्ने ।

९. खाता खोल्दा स्वतः(Default)प्राप्त हुने पासवर्डलाई तत्काल परिवर्तन गर्ने ।

१०. आफ्नो पासवर्ड, ओटिपी, पिन कोड अन्यलाई उपलब्ध नगराउने ।

११. आफ्नो खातालाई सुरक्षित राख्न प्रमाणीकरण (ओटिपी, फिङ्गर तथा अनुहार स्क्यान,पिन कोड लगायत अन्य अनुमति) विधि(Multi Level Authentication)को प्रयोग गर्ने ।

१२. पासवर्ड व्यवस्थापनको लागि पासवर्ड म्यानेजरको व्यवस्थापन गर्ने ।

**खण्ड३**

**अभिलेख व्यवस्थापन तथा सुरक्षा**

## १०. अभिलेख व्यवस्थापन तथा सुरक्षा

१. कम्प्यूटर तथा ल्यापटपको सिस्टम ड्राइभ (System Drive)मा फाइलहरु नराख्ने ।

२. अभिलेखको प्रकृति बमोजिमका फोल्डरहरु बनाईत्यसभित्र फाइलहरु राख्ने ।

३. अभिलेखको गोपनियताको स्तर बमोजिम फोल्डर एंव फाइलहरुमा पासवर्ड राख्ने ।

४. डकुमेण्टको संवेदनशिलताको आधारमा सम्बन्धित निकायमा अभिलेखको डिजिटल प्रति पेश गर्दा उक्त फाइलमा पासवर्ड राखि पठाउने ।

५. संस्थागत फाइल तथा अभिलेखहरु आदान प्रदान गर्दा सुरक्षित प्लेटफमको प्रयोग गर्ने ।

६. सामाजिक संजालका माध्यमबाट संस्थागत फाइल तथा विवरणहरु आदान प्रदान नगर्ने ।

**खण्ड ४**

**इमेल तथा इन्टरनेट संचालन तथा प्रयोग**

## ११. इमेल तथा इन्टरनेट संचालन तथा प्रयोग

१. संस्थागत प्रयोजनका लागि छुट्टै इमेल खाता खोल्ने ।

२. इमेल सेवा प्रदायकले उपलब्ध गराएको Security Feature लाई सधैंEnable गर्ने ।

३. संस्थागत प्रयोजन बाहेकका अपरिचित व्यक्ति, संस्था वा खाताबाट आएको इमेल, लिंक वा फाइल नखोल्ने, स्पाम र जंक इमेल नखोल्ने ।

४. स्पाम र जंक इमेललाई ७ दिनमा डिलिट गर्ने ।

५. संकास्पद इमेललाई डिलिट गरी उक्त इमेल ठेगानालाई बल्क गर्ने ।

६. इमेल मार्फत आएका .EXE, .PIF, .APPLICATION, .GADGET, .MSI, .MSP, .COM, .SCR, .HTA, .CPL,.VBS जस्ता एस्टेन्सन भएका फाइलहरु नखोल्ने ।

७. वेवसाइटको विश्वसनियता निक्यौल नगरी संस्थागत तथा व्यक्तिगत विवरणहरु उपलब्ध नगराउने ।

८. अनावश्यक साइटमा लगइन नगर्ने ।

९. अनावश्यक साइट, व्यक्ति, इभेन्ट, कार्यक्रम, सामाजिक संजालका पेजलाई सब्बक्राइव, लाइकतथा फलो नगर्ने ।

१०. संस्थागत समाजिक संजालका पेजहरूमार्फत हुन सक्ने साईवर आक्रमणलाई रोक्नओटिपी, फिङ्गर तथा अनुहार स्क्यान,पिन कोड लगायत Multi Level Authenticationजस्ता सुरक्षा प्रणाली अवलम्बन गर्ने ।

११. शंकास्पद इमेलको रेस्पोन्स गर्नुपर्ने भएमा आधिकारिता पुष्टि गरीआईटि विभाग वा सो सँग सम्बन्धित कर्मचारीको परामर्श पश्चात मात्र रेस्पोन्स गर्ने ।

## खण्ड ५
## वाइफाइ संचालन तथा व्यवस्थापन

### १२. वाइफाइ संचालन तथा व्यवस्थापन

१. कार्यालयमा वाइफाइ जडान गरेपश्चात वाइफाइमा रहेको डिफल्ट (Default) यूजरनेमर पासवर्ड तत्काल परिवर्तन गर्ने ।

२. वाइफाइ सेवा प्रदायकबाट प्राप्त हुने डिफल्ट सर्भिस सेट आर्डन्टिफायर (SSID) परिवर्तन गरी उक्त (SSID) लाई हाइड गर्ने ।

३. वायरलेस राउटर(Router) लाई नियमित रुपमा अद्यावधिक गर्ने ।

४. कार्यालयको संवेदनशील कार्यमा प्रयोग हुने राउटरको पासवर्ड अन्यलाई उपलब्ध नगराउने । कथमकदाचित उपलब्ध गराउनुपर्ने भएमा छुट्टै राउटर मार्फत उपलब्ध गराउने ।

५. कार्यालय बन्द रहने समयमा राउटर अफ गर्ने ।

६. सार्वजनिक स्थानको निःशुल्क वाइफाई कार्यालयको उपकरणमा लगइन नगर्ने । व्यक्तिगत प्रयोजनमा समेत निःशुल्क वाइफाईको प्रयोगलाई निरुत्साहित गर्ने ।

७. सार्वजनिक स्थानमा इन्टरनेटको आवश्यकता भएमाडाटाको मात्र प्रयोग गर्ने ।

## खण्ड ६
## अनलाइन बैकिङ्ग एप्लिकेशनको प्रयोग

### १३. अनलाइन बैकिङ्ग एप्लिकेशनको प्रयोग

१. अनलाइन बैकिङ्गका लागि आधिकारीक वेबसाइट र मोबाइल बैकिङ्गका लागि आधिकारीक एप्लिकेशनको मात्र प्रयोग गर्ने ।

२. अनलाइन बैकिङ्गमा प्रयोग हुने उपकरणहरुमा अनिवार्य रुपमा पासवर्डलक, प्याटनलक, पिनलक तथा वायोमेट्रिकलक राख्ने ।

३. अनलाइन बैकिङ्गका लागि वेबसाइटको प्रयोग गर्दा सोको पूरा नाम (URL) टाइप गर्ने र कुनै लिङ्क मार्फत उक्त वेबसाइट नखोल्ने ।

४. अनलाइन कारोबारका लागि नोटिफिकेशनलाई अनिवार्य गर्ने ।

५. बैकिङ्ग कारोबारको ओटिपी, पिनकोड र पासवर्ड कसैलाई शेयर नगर्ने।

६. अनलाइन बैकिङ्ग खाताको यूजरनेम र पासवर्ड वेबसाइट वा एप्लिकेशनमा सेभ नगर्ने ।

७. अनलाइन बैकिङ्ग खाताको यूजरनेम र पासवर्ड समय समयमा परिवर्तन गर्ने ।

## खण्ड ७
## विविध

### १४ संशोधन, व्याख्या, लागु तथा परिमार्जन :

१. यो मार्गदर्शनको संशोधन र परिमार्जन गर्ने अधिकार महासंघको साधारण सभामा निहित हुनेछ ।

२. यो मार्गदर्शनको अन्तिम व्याख्या गर्ने अधिकार महासंघको संचालक समितिमा निहित हुनेछ ।

३. यो मार्गदर्शनका बुँदाहरू साईवर सुरक्षा नीति, सहकारी ऐन, नियमावली र महासंघको विनियमसँग बाँझिन गएमा बाँझिएको हदसम्म स्वत: खारेज हुनेछ ।