বাংলাদেশ কৃষি ব্যাংক
প্রধান কার্যালয়, ঢাকা
ভিজিলেন্স স্কোয়াড বিভাগ
(সাইবার সিকিউরিটি ইউনিট)

ফোনঃ ০২২২৩৩৮০০৩৬
০২২২৩৩৫৮৬৮০
ইমেইলঃdgmvsd@krishibank.org.bd

স্মারক নং-প্রকা/ভিএসডি/সিএসইউ-৪৫/২০২৩-২০২৪/৭১১

তারিখঃ ০১-০৪-২০২৪ খ্রিঃ

মহাব্যবস্থাপক , সকল বিভাগীয় কার্যালয়/ স্থানীয় মুখ্য কার্যালয়
অধ্যক্ষ, বিকেবি স্টাফ কলেজ
সকল উপমহাব্যবস্থাপক/ সচিব/ বিভাগীয় প্রধান, প্রধান কার্যালয়
বিভাগীয় নিরীক্ষা কর্মকর্তা, সকল বিভাগীয় নিরীক্ষা কার্যালয়
উপমহাব্যবস্থাপক, সকল কর্পোরেট শাখা
মুখ্য আঞ্চলিক/ আঞ্চলিক ব্যবস্থাপক, সকল মুখ্য আঞ্চলিক/ আঞ্চলিক কার্যালয়
আঞ্চলিক নিরীক্ষা কর্মকর্তা, সকল আঞ্চলিক নিরীক্ষা কার্যালয়
শাখা ব্যবস্থাপক, সকল শাখা
বাংলাদেশ কৃষি ব্যাংক।

বিষয়ঃ <u>বাংলাদেশ কৃষি ব্যাংকের সাইবার নিরাপত্তা নিশ্চিত করার লক্ষ্যে Cyber নিরাপত্তা ঝুঁকি মোকাবেলায় করণীয় প্রসঙ্গে।</u>

মহোদয়,

উপর্যুক্ত বিষয়ের প্রতি সদয় দৃষ্টি আকর্ষণ করা হলো।

০২। প্রযুক্তির উৎকর্ষ, উন্নত ও আধুনিক গ্রাহক সেবা প্রদানের লক্ষ্যে বর্তমানে বাংলাদেশ কৃষি ব্যাংকের সকল শাখায় (বর্তমানে ১০৩৮ টি শাখা ও ৩ টি উপশাখা) Online Banking, BACH, EFTN, SWIFT, Remittance, RTGS, ATM, Email Service, SMS Service সহ অন্যান্য সেবা কার্যক্রম ডিজিটাল প্রযুক্তির মাধ্যমে সম্পন্ন হচ্ছে। ডিজিটাল প্রযুক্তির মাধ্যমে পরিচালিত হওয়ায় ব্যাংকের সম্ভাব্য সাইবার নিরাপত্তা সংশ্লিষ্ট ঝুঁকি বিবেচনা করে আইসিটি বিষয়ক সকল জাল-জালিয়াতি ও দুর্নীতি রোধ কল্পে অত্র ব্যাংকের ভিজিলেন্স স্কোয়াড বিভাগের অধীনে সাইবার সিকিউরিটি ইউনিট (Cyber Security Unit) গঠন করা হয়।

০৩। ব্যাংক এবং আর্থিক প্রতিষ্ঠানসমূহে ডিজিটাল/আধুনিক ব্যাংকিং সেবা বৃদ্ধির পাশাপাশি সাম্প্রতিক সময়ে ব্যাংক এবং আর্থিক প্রতিষ্ঠানসমূহে ক্রমবর্ধমানভাবে সাইবার নিরাপত্তা ঝুঁকিও বৃদ্ধি পাচ্ছে। তদপ্রেক্ষিতে অত্র ব্যাংকের সাইবার নিরাপত্তা ঝুঁকি নিরসন ও মোকাবেলার লক্ষ্যে আইসিটি মহাবিভাগ থেকে সময়ে সময়ে জারিকৃত বিভিন্ন পরিপত্র/সার্কুলার/গাইডলাইন সহ বাংলাদেশ ব্যাংক হতে জারিকৃত আইসিটি সিকিউরিটি গাইডলাইন ২০২৩ যথাযথভাবে পরিপালনের জন্য ব্যবস্থাপনা পরিচালক মহোদয় কর্তৃক নিম্নোক্ত নির্দেশনা প্রদান করা হয়ঃ

(i) অত্র সার্কুলার জারির পরপরই শাখা/কার্যালয়ে ব্যবহৃত সকল কম্পিউটার, সার্ভারসহ ব্যাংকের সার্ভিস প্রদানে ব্যবহৃত সকল এপ্লিকেশন/সফটওয়্যার-এর পাসওয়ার্ড পরিবর্তন করতে হবে।

(ii) নিজের ব্যবহৃত পাসওয়ার্ড অন্য কারও নিকট প্রকাশ করা যাবে না।

(iii) কম্পিউটারের অপারেটিং সিস্টেম, এপ্লিকেশন/সফটওয়্যার-এ ব্যবহারকারীর সকল একাউন্টের জন্য শক্তিশালী ও জটিল পাসওয়ার্ড ব্যবহার করতে হবে। পাসওয়ার্ড ব্যবহারের ক্ষেত্রে সর্বনিম্ন ১১ ক্যারেক্টার (Uppercase(A-Z), Lowercase(a-z), Alphanumeric (0-9), Special Character যেমন- !@#$%&*_ ইত্যাদি) ব্যবহার করতে হবে।

(iv) সময়ে সময়ে ব্যবহৃত পাসওয়ার্ড পরিবর্তন নিশ্চিত করতে হবে।

(v) ব্যাংকের কাজে ব্যবহৃত email/ Network/ Software/ Database কোন ব্যক্তিগত কাজে ব্যবহার করা যাবে না।

(vi) অপরিচিত/ অনাকাঙ্ক্ষিত/ সন্দেহজনক ঠিকানা হতে আগত ই-মেইলের কোন লিংকে ক্লিক করা যাবে না এবং সংযুক্ত কোন pdf বা অন্যান্য ফাইল ডাউনলোড করা যাবে না।

(vii) সকল কম্পিউটার/সার্ভারে অপারেটিং সিস্টেম, এপ্লিকেশন এবং অন্যান্য সফটওয়্যার নিয়মিতভাবে আপডেট করতে হবে।

(viii) অফিস সময়ের পর কম্পিউটার, প্রিন্টার, ইউপিএস সহ অন্যান্য ডিভাইসসমূহ সঠিকভাবে বন্ধ করতে হবে।

(ix) ব্যাংকের কাজে ব্যবহৃত কম্পিউটার/ সার্ভার সমূহে অনুমোদিত Antivirus ব্যবহার করা এবং Antivirus নিয়মিত Update করার পাশাপাশি নির্দিষ্ট সময় পরপর ডিভাইসসমূহ Antivirus দ্বারা Scan করতে হবে।

(x) ব্যাংকের কম্পিউটার ও নেটওয়ার্ক এ কোন Pendrive, মোবাইল, পোর্টেবল হার্ডডিস্ক বা অন্যান্য অননুমোদিত ডিভাইস সংযুক্ত করা যাবে না।

(xi) কম্পিউটারের প্রয়োজনীয় ডাটা Backup রাখতে হবে।

(xii) সার্ভারসমূহের এপ্লিকেশন ও Database নিয়মিত Backup রাখতে হবে।

(xiii) ইন্টারনেট সংযুক্ত কম্পিউটার ব্যবহার করে কোন ব্যক্তিগত কাজ করা থেকে বিরত থাকতে হবে। পাশাপাশি ব্যাংকের কাজের সাথে সংশ্লিষ্ট নয় এমন Website ব্রাউজ করা থেকে বিরত থাকতে হবে।

(xiv) অননুমোদিত কোন অপারেটিং সিস্টেম/ সফটওয়্যার/ Browser Extension ইন্সটল বা ব্যবহার করা থেকে বিরত থাকতে হবে।

(xv) কম্পিউটার/ সার্ভার সমূহে নিজস্ব firewall on রাখতে হবে।

(xvi) CBS এর কাজে ব্যবহৃত কম্পিউটারে কোনভাবেই ইন্টারনেট ব্যবহার করা যাবে না।

(xvii) CBS এর কাজে ব্যবহৃত কম্পিউটারে CBS সংশ্লিষ্ট কাজ ব্যতীত অন্য কোন কাজ করা যাবে না।

(xviii) কম্পিউটার/ সার্ভারের Remote Connection (RDP) বন্ধ রাখতে হবে।

(xix) ব্যাংকের গুরুত্বপূর্ন অবকাঠামো/ Network/ Software এ ছবি/ স্ক্রিনশট/ ভিডিও / ডায়াগ্রাম সামাজিক যোগাযোগ মাধ্যমসহ অননুমোদিত স্থানে প্রকাশ/ প্রচার থেকে বিরত থাকতে হবে।

(xx) Hardware/ Software/ Network এর Maintenance এর জন্য ভেন্ডর প্রতিষ্ঠান হতে আগত ব্যক্তির পরিচিতি নিশ্চিত হয়ে সার্ভিস গ্রহণ করতে হবে।

০৪। এমতাবস্থায় ব্যাংকের সাইবার ঝুঁকি নিরসন ও মোকাবেলার লক্ষ্যে উপরে উল্লিখিত নির্দেশনাসমূহ যথাযথভাবে পরিপালনের জন্য আপনাদেরকে অনুরোধ করা হলো ।

অনুমোদনক্রমে-

০১.০৪.২০২৪ খ্রিঃ

(মোঃ সাখাওয়াত হোসেন)
উপমহাব্যবস্থাপক

স্মারক নং-প্রকা/ভিএসডি/সিএসইউ-৪৫/২০২৩-২০২৪/৭১১ তারিখঃ ০১-০৪-২০২৪ খ্রিঃ

<u>সদয় অবগতি ও জ্ঞাতার্থে অনুলিপিঃ</u>

০১। চীফ স্টাফ অফিসার, ব্যবস্থাপনা পরিচালক মহোদয়ের সচিবালয়, বিকেবি, প্রকা, ঢাকা।

০২। স্টাফ অফিসার, উপব্যবস্থাপনা পরিচালক-১/২/৩ মহোদয়ের সচিবালয়, বিকেবি, প্রকা, ঢাকা।

০৩। স্টাফ অফিসার, সকল মহাব্যবস্থাপক মহোদয়ের দপ্তর, বিকেবি, প্রকা, ঢাকা।

০৪। উপমহাব্যবস্থাপক, আইসিটি সিস্টেমস বিভাগ, বিকেবি, প্রকা, ঢাকা (বর্ণিত পত্রটি ব্যাংকের অফিসিয়াল ওয়েবসাইটে আপলোড করার প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য অনুরোধ করা হলো) ।

০৫। নথি।

০১/০৪/২০২৪ খ্রিঃ

(মোঃশরীফুল ইসলাম ভূইয়া)
সহকারী মহাব্যবস্থাপক
(Cyber Security Unit)