ডিজিটাল সুরক্ষা নির্দেশিকা, ২০২২
(ব্যবহারকারীদের জন্য)
সংস্করণ ১.০

আইসিটি সেল
অর্থনৈতিক সম্পর্ক বিভাগ
অর্থ মন্ত্রণালয়

পৌষ ১৪২৯/ডিসেম্বর ২০২২

১. প্রেক্ষাপট:

তথ্য-প্রযুক্তি নির্ভর বিশ্বায়নের যুগে মানুষের দোরগোড়ায় সেবা পৌঁছে দিতে প্রধানতম একটি মাধ্যম হলো ইন্টারনেট। দৈনন্দিন জীবনে তথ্যপ্রযুক্তি ও ইন্টারনেটের নির্ভরশীলতা বাড়ার সঙ্গে সঙ্গে কম্পিউটার ও ইন্টারনেটে রক্ষিত দাপ্তরিক ও গুরুত্বপূর্ণ তথ্যসমূহের নিরাপত্তার ঝুঁকিও বৃদ্ধি পেয়েছে। সচিবালয় নির্দেশমালা, ২০১৪-এ সাইবার নিরাপত্তা ও তথ্য নিরাপত্তার ওপর গরুত্বারোপ করা হয়েছে। ডিজিটাল বাংলাদেশ অর্থাৎ রূপকল্প ২০২১ বাস্তবায়নে তথ্য-উপাত্ত ডিজিটাইজেশনের সঙ্গে সঙ্গে এর নিরাপত্তা বিধানের প্রতি সর্বোচ্চ সতর্কতা অবলম্বন জরুরি হয়ে পড়েছে।

নিরাপদ ইন্টারনেট ব্রাউজিং-এর কলাকৌশল না জেনে ইন্টারনেট ব্যবহার করার ফলে সম্প্রতি সরকারি দপ্তরসমূহে ব্যবহৃত অনলাইন সিস্টেম, ডিজিটাল ডিভাইস ও ডিভাইসে সংরক্ষিত গুরুত্বপূর্ণ তথ্যসমূহ বিভিন্ন ধরণের সাইবার আক্রমণের শিকার হচ্ছে। এ লক্ষ্যে অর্থনৈতিক সম্পর্ক বিভাগের ডিজিটাল ডিভাইস ও তথ্য সুষ্ঠুভাবে সংরক্ষণসহ নিরাপত্তা ব্যবস্থা গ্রহণের জন্য 'ডিজিটাল সুরক্ষা নির্দেশিকা, ২০২২' প্রণয়ন করা হলো। এ নির্দেশিকা অনুসরণের মাধ্যমে ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তার সঙ্গে সংশ্লিষ্ট কর্মকর্তা-কর্মচারীগণ নিরাপত্তায় অধিকতর দায়িত্বশীল ভূমিকা পালন করতে সক্ষম হবেন।

২. ডিজিটাল ডিভাইস ব্যবহারে করণীয়:

(ক) কম্পিউটার/ল্যাপটপ/ট্যাব/মোবাইল ইত্যাদি ডিজিটাল ডিভাইসসমূহ অবশ্যই পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;

(খ) দাপ্তরিক কম্পিউটার/ল্যাপটপে আইসিটি সেলের পরামর্শ ব্যতীত কোন ধরনের সফটওয়্যার ইন্সটল না করা;

(গ) কম্পিউটার/ল্যাপটপে সংরক্ষিত গুরুত্বপূর্ণ ফাইল সমূহ zip করে ব্যাকআপ রাখা;

(ঘ) ব্যাকআপ ফাইলসমূহ অপারেটিং সিস্টেম ড্রাইভ (c:/, ডেস্কটপ, ডাউনলোড ইত্যাদি) ব্যতীত অন্য ড্রাইভে সংরক্ষণ করা;

(ঙ) ডাটা ট্রান্সফারের ক্ষেত্রে পেনড্রাইভসহ এক্সটার্নাল হার্ডডিস্ক, মেমরি কার্ড, সিডি/ডিভিডি ডিস্ক ইত্যাদির পরিবর্তে ই-মেইল/ ক্লাউড সার্ভিস/ ফাইল সার্ভার ব্যবহার করা;

(চ) দাপ্তরিক ডেস্কটপ/ল্যাপটপে ভিজিটরের কোন ডিভাইস (পেনড্রাইভ, মোবাইল, এক্সটার্নাল হার্ডডিস্ক, মেমরি কার্ড, সিডি/ডিভিডি ডিস্ক ইত্যাদি) সিস্টেমে সংযুক্ত না করা;

(ছ) সার্ভার/ কম্পিউটার/ল্যাপটপের কোন ড্রাইভ, ফোল্ডার, ফাইল, ইত্যাদি অননুমোদিত কারও সঙ্গে শেয়ার না করা;

(জ) ডিজিটাল ডিভাইসে Biometric Authentication (Fingerprint, Scans Option ইত্যাদি) থাকলে তা Enable রাখা;

(ঝ) কম্পিউটার/ল্যাপটপ/মোবাইলে অপ্রয়োজনীয় Service চালু না করা;

(ঞ) অপারেটিং সিস্টেম নিয়মিত আপডেট রাখা;

(ট) ডিজিটাল ডিভাইসে রিমোট অ্যাকসেস প্রদান না করা;

(ঠ) গুরুত্বপূর্ণ ডকুমেন্টসসমূহ পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;

(ড) অপারেটিং সিস্টেমে ফায়ারওয়াল বন্ধ না রাখা;

(ঢ) প্রয়োজন না হলে ডিভাইসের সাথে সংযুক্ত যোগাযোগ মাধ্যম (ব্লু-টুথ, ওয়াই-ফাই, হটস্পট, ইনফ্রারেড ইত্যাদি) বন্ধ রাখা;

(ণ) নিয়মিত ডিজিটাল ডিভাইস পরিষ্কার পরিচ্ছন্ন রাখা;

(ত) ডেস্ক থেকে উঠে যাবার সময় ব্যবহৃত কম্পিউটার/ল্যাপটপ সিস্টেম লক/ লগ আউট করে যাওয়া এবং কাজ শেষে/ অফিস ত্যাগের পূর্বে কম্পিউটার/ল্যাপটপ shut down করা।

৩. পাসওয়ার্ড ব্যবস্থাপনায় করণীয়:

(ক) ব্যবহৃত পাসওয়ার্ড কমপক্ষে ৮ ডিজিট হওয়া সমীচীন। পাসওয়ার্ড কমপক্ষে একটি বড় অক্ষর, একটি ছোট অক্ষর, সংখ্যা ও বিশেষ চিহ্নের সমন্বয়ে থাকা প্রয়োজন;

(খ) অন্য কোনো ব্যক্তির সঙ্গে ব্যবহৃত পাওয়ার্ডটি শেয়ার না করা এবং কেউ জানতে পারে এমন কোথাও লিখে না রাখা;

(গ) পাসওয়ার্ড তৈরিতে নিজের নাম, জন্ম তারিখ ও অন্যান্য ব্যক্তিগত তথ্য ব্যবহারে বিরত থাকা;

(ঘ) নিয়মিত (অন্তত ২/৩ মাস পর পর) পাসওয়ার্ড পরিবর্তন করা;

(ঙ) ব্রাউজারে পাসওয়ার্ড স্থায়ীভাবে সংরক্ষণ না করা;

৪. ইন্টারনেট ব্যবহারে করণীয়:

(ক) টরেন্ট, ফ্রি প্রক্সি, পর্নো, ডেটিং, জুয়া/ ক্যাসিনো, বেটিং, লটারি, জঙ্গিবাদ ইত্যাদি অনৈতিক সাইট ব্যবহার না করা;

(খ) ইন্টারনেট সংযোগের ক্ষেত্রে অননুমোদিত ডিভাইস ব্যবহার না করা;

(গ) ব্রাউজার হিস্ট্রি ও কম্পিউটার ক্যাশ মেমরি নিয়তি পরিষ্কার করা;

(ঘ) নিয়মিত ব্রাউজার আপডেট রাখা;

৫. ই-মেইল ব্যবস্থাপনায় করণীয়:

(ক) দাপ্তরিক কাজে সরকারি ই-মেইল ব্যবহার নিশ্চিত করা;

(খ) শুধুমাত্র দাপ্তরিক কাজের জন্য অফিসিয়াল ই-মেইল ব্যবহার করা;

(গ) ই-মেইল ব্যবহার শেষে লগ আউট করা;

(ঘ) ভাইরাস বা ম্যালওয়্যার থেকে সুরক্ষায় ই-মেইলে আগত .exe, .bat, .vbs, .scr ইত্যাদি ফাইল খোলা থেকে বিরত থাকা;

(ঙ) সন্দেহজনক ই-মেইল বা সংযুক্তি (Attachment) না খোলা;

(চ) ই-মেইল থেকে নিয়মিত অপ্রয়োজনীয় তথ্যাদি অপসারণ করা;

(ছ) খুব বেশি জরুরি না হলে অন্যের কম্পিউটার থেকে ই-মেইল, সোস্যাল মিডিয়া প্ল্যাটফর্ম ইত্যাদিতে লগ-ইন করা থেকে বিরত থাকা;

(ছ) ই-মেইলে আগত অবাঞ্ছিত মেইল, স্পট অফার, লটারি মানি, ফ্রি লোন, এ্যাওয়ার্ড ইত্যাদি নানা ধরনের আকর্ষণীয়, প্রণোদনামূলক মেইলে ক্লিক না করে তাৎক্ষণিকভাবে এ সকল ই-মেইল ডিলিট করে দেওয়া;

(জ) সরকারি ই-মেইল নীতিমালা ২০১৮ অনুসরণ করা;

৬. সামাজিক যোগযোগ মাধ্যম ব্যবহারে করণীয়:

(ক) অফিস চলাকালীন সময়ে সামাজিক যোগাযোগ মাধ্যম ব্যবহার সীমিত করা;

(খ) সামাজিক যোগাযোগের বিভিন্ন মাধ্যমে সরকার বা রাষ্ট্রের ভাবমূর্তি ক্ষুন্ন হয় এমন কোনো পোস্ট /আপলোড, কমেন্ট, লাইক শেয়ার করা থেকে বিরত থাকা;

(গ) সামাজিক যোগাযোগ মাধ্যমসহ অন্য কোন ব্যক্তিগত একাউন্ট খোলার ক্ষেত্রে অফিসিয়াল ই-মেইল ব্যবহার না করা;

(ঘ) সরকারি প্রতিষ্ঠানে সামাজিক যোগযোগ মাধ্যম ব্যবহার সংক্রান্ত নির্দেশিকা, ২০১৯ (পরিমার্জিত সংস্করণ) অনুসরণ করা;

৭. তথ্য নিরাপত্তার আইনগত বিষয়সমূহ:

তথ্য নিরাপত্তার সাথে সংশ্লিষ্ট বিভিন্ন আইন ও বিধি-বিধান সম্পর্কে সচেতন থেকে সকলকে দায়িত্ব পালন করতে হবে। এ ক্ষেত্রে নিম্নোক্ত আইন, বিধি-বিধান, নীতিমালা ও গাইডলাইন ছাড়াও সংশ্লিষ্ট অন্যান্য আইন ও বিধি-বিধানের প্রতি লক্ষ্য রাখতে হবে:

১. সচিবালয় নির্দেশমালা, ২০১৪;

২. Government of Bangladesh Information Security Manual, 2016

৩. তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা, ২০১৮;

৪. ডিজিটাল নিরাপত্তা আইন, ২০১৮;

৫. সরকারি চাকরি আইন, ২০১৮;

৬. সরকারি ই-মেইল নীতিমালা, ২০১৮

৭. সরকারি প্রতিষ্ঠানে সামাজিক যোগযোগ মাধ্যম ব্যবহার সংক্রান্ত নির্দেশিকা, ২০১৯ (পরিমার্জিত সংস্করণ)

৮. ডিজিটাল ডিভাইস, ইন্টারনেট এবং তথ্য রক্ষণাবেক্ষণ ও নিরাপত্তা নির্দেশিকা, ২০২০