কৃষিই সমৃদ্ধি

অতি জরুরি
ই-মেইল মারফত

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
কৃষি মন্ত্রণালয়
নীতি-১ শাখা
www.moa.gov.bd

স্মারক নং-১২.০০.০০০০.০৭৫.২২.০৪৭.১৯. ১৩৮

তারিখ : ২৭/০৭/১৪২৬ ব:
১২/১১/২০১৯ খ্রি:

বিষয়: 'ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা'-এর খসড়ার ওপর মতামত প্রেরণ।

সূত্র: মন্ত্রিপরিষদ বিভাগ (ই-গভর্নেন্স-১ অধিশাখা) এর স্মারক নম্বর: ০৪.০০.০০০০.৮৩১.২২.০০৩.১৯.৫৮; তারিখ: ৩০ অক্টোবর ২০১৯

উপর্যুক্ত বিষয়ের প্রেক্ষিতে জানানো যাচ্ছে যে, মন্ত্রিপরিষদ বিভাগ কর্তৃক প্রেরিত পত্রের অনুলিপি এতদসঙ্গে প্রেরণ করা হলো। সকল সরকারি কার্যালয়ে ব্যবহারের জন্য সমন্বিত ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা, ২০১৯-এর খসড়া প্রণয়ন করা হয়েছে। আগামী ২০ নভেম্বর ২০১৯ তারিখের মধ্যে উক্ত খসড়া নির্দেশিকার ওপর মতামত প্রেরণের জন্য অনুরোধ করা হয়েছে।

০২। বর্ণিতাবস্থায়, উক্ত বিষয়ের উপর আগামী ০৩ কর্ম দিবসের মধ্যে মতামত প্রদানের জন্য নির্দেশক্রমে অনুরোধ করা হলো।

সংযুক্তি: বর্ণনামতে।

(মোঃ হানিফ উদ্দিন)
উপসচিব
ফোন: ৯৫৪০৩৮৫
ই-মেইল: moapolicy1@gmail.com

বিতরণ (জ্যেষ্ঠতার ভিত্তিতে নয়) :

১) নির্বাহী চেয়ারম্যান, বাংলাদেশ কৃষি গবেষণা কাউন্সিল, ফার্মগেট, ঢাকা।
২) চেয়ারম্যান, বাংলাদেশ কৃষি উন্নয়ন কর্পোরেশন, কৃষি ভবন, ৪৯-৫১ মতিঝিল বা/এ, ঢাকা।
৩) মহাপরিচালক, কৃষি বিপণন অধিদপ্তর, খামারবাড়ি, ঢাকা।
৪) মহাপরিচালক, কৃষি সম্প্রসারণ অধিদপ্তর, খামারবাড়ি, ঢাকা।
৫) মহাপরিচালক, বাংলাদেশ ধান গবেষণা ইনস্টিটিউট, জয়দেবপুর, গাজীপুর।
৬) মহাপরিচালক, বাংলাদেশ পাট গবেষণা ইনস্টিটিউট, মানিক মিয়া এভিনিউ, ঢাকা।
৭) মহাপরিচালক, জাতীয় কৃষি প্রশিক্ষণ একাডেমি (নাটা), গাজীপুর।
৮) মহাপরিচালক, বাংলাদেশ কৃষি গবেষণা ইনস্টিটিউট, জয়দেবপুর, গাজীপুর।
৯) মহাপরিচালক, বাংলাদেশ সুগারক্রপ গবেষণা ইনস্টিটিউট, ঈশ্বরদী, পাবনা।
১০) মহাপরিচালক, বাংলাদেশ পরমানু কৃষি গবেষণা ইনস্টিটিউট (বিনা), ময়মনসিংহ।
১১) মহাপরিচালক, বাংলাদেশ গম ও ভুট্টা গবেষণা ইনস্টিটিউট, নশিপুর, দিনাজপুর।
১২) ব্যবস্থাপনা পরিচালক, হর্টেক্স ফাউন্ডেশন, সেচ ভবন (৩য় তলা), মানিক মিয়া এভিনিউ, ঢাকা।
১৩) পরিচালক, মৃত্তিকা সম্পদ উন্নয়ন ইনস্টিটিউট, মৃত্তিকা ভবন, ফার্মগেট, ঢাকা।
১৪) নির্বাহী পরিচালক, বাংলাদেশ ফলিত পুষ্টি গবেষণা ও প্রশিক্ষণ ইনস্টিটিউট (বারটান), সেচ ভবন, মানিকমিয়া এভিনিউ, ঢাকা।
১৫) নির্বাহী পরিচালক, বরেন্দ্র বহুমুখী উন্নয়ন কর্তৃপক্ষ, রাজশাহী।
১৬) নির্বাহী পরিচালক, তুলা উন্নয়ন বোর্ড, খামারবাড়ি, ঢাকা।
১৭) পরিচালক, বীজ প্রত্যয়ন এজেন্সী, জয়দেবপুর, গাজীপুর।
১৮) পরিচালক, কৃষি তথ্য সার্ভিস, খামারবাড়ি, ফার্মগেট, ঢাকা।

অনুলিপি:

১। অতিরিক্ত সচিব (পিপিসি) মহোদয়ের ব্যক্তিগত কর্মকর্তা, কৃষি মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা।
২। অতিরিক্ত সচিব (পিপিবি) মহোদয়ের ব্যক্তিগত কর্মকর্তা, কৃষি মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা।
৩। অফিস কপি।

কৃষিই সমৃদ্ধি

অতি জরুরি
ই-মেইল মারফত

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
কৃষি মন্ত্রণালয়
নীতি-১ শাখা
www.moa.gov.bd

স্মারক নং-১২.০০.০০০০.০৭৫.২২.০৪৭.১৯. ১৩৮

তারিখ : ২৭/০৭/১৪২৬ ব:
১২/১১/২০১৯ খ্রি:

বিষয়: 'ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা'-এর খসড়ার ওপর মতামত প্রেরণ।

সূত্র: মন্ত্রিপরিষদ বিভাগ (ই-গভর্নেন্স-১ অধিশাখা) এর স্মারক নম্বর: ০৪.০০.০০০০.৮৩১.২২.০০৩.১৯.৫৮; তারিখ: ৩০ অক্টোবর ২০১৯

উপর্যুক্ত বিষয়ের প্রেক্ষিতে জানানো যাচ্ছে যে, মন্ত্রিপরিষদ বিভাগ কর্তৃক প্রেরিত পত্রের অনুলিপি এতদসঙ্গে প্রেরণ করা হলো। সকল সরকারি কার্যালয়ে ব্যবহারের জন্য সমন্বিত ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা, ২০১৯-এর খসড়া প্রণয়ন করা হয়েছে। আগামী ২০ নভেম্বর ২০১৯ তারিখের মধ্যে উক্ত খসড়া নির্দেশিকার ওপর মতামত প্রেরণের জন্য অনুরোধ করা হয়েছে।

০২। বর্ণিতাবস্থায়, উক্ত বিষয়ের উপর আগামী ০৩ কর্ম দিবসের মধ্যে মতামত প্রদানের জন্য নির্দেশক্রমে অনুরোধ করা হলো।

সংযুক্তি: বর্ণনামতে।

(মোঃ হানিফ উদ্দিন)
উপসচিব
ফোন: ৯৫৪০৩৮৫
ই-মেইল: moapolicy1@gmail.com

বিতরণ (জ্যেষ্ঠতার ভিত্তিতে নয়) :

১) নির্বাহী চেয়ারম্যান, বাংলাদেশ কৃষি গবেষণা কাউন্সিল, ফার্মগেট, ঢাকা।
২) চেয়ারম্যান, বাংলাদেশ কৃষি উন্নয়ন কর্পোরেশন, কৃষি ভবন, ৪৯-৫১ মতিঝিল বা/এ, ঢাকা।
৩) মহাপরিচালক, কৃষি বিপণন অধিদপ্তর, খামারবাড়ি, ঢাকা।
৪) মহাপরিচালক, কৃষি সম্প্রসারণ অধিদপ্তর, খামারবাড়ি, ঢাকা।
৫) মহাপরিচালক, বাংলাদেশ ধান গবেষণা ইনস্টিটিউট, জয়দেবপুর, গাজীপুর।
৬) মহাপরিচালক, বাংলাদেশ পাট গবেষণা ইনস্টিটিউট, মানিক মিয়া এভিনিউ, ঢাকা।
৭) মহাপরিচালক, জাতীয় কৃষি প্রশিক্ষণ একাডেমি (নাটা), গাজীপুর।
৮) মহাপরিচালক, বাংলাদেশ কৃষি গবেষণা ইনস্টিটিউট, জয়দেবপুর, গাজীপুর।
৯) মহাপরিচালক, বাংলাদেশ সুগারক্রপ গবেষণা ইনস্টিটিউট, ঈশ্বরদী, পাবনা।
১০) মহাপরিচালক, বাংলাদেশ পরমানু কৃষি গবেষণা ইনস্টিটিউট (বিনা), ময়মনসিংহ।
১১) মহাপরিচালক, বাংলাদেশ গম ও ভুট্টা গবেষণা ইনস্টিটিউট, নশিপুর, দিনাজপুর।
১২) ব্যবস্থাপনা পরিচালক, হর্টেক্স ফাউন্ডেশন, সেচ ভবন (৩য় তলা), মানিক মিয়া এভিনিউ, ঢাকা।
১৩) পরিচালক, মৃত্তিকা সম্পদ উন্নয়ন ইনস্টিটিউট, মৃত্তিকা ভবন, ফার্মগেট, ঢাকা।
১৪) নির্বাহী পরিচালক, বাংলাদেশ ফলিত পুষ্টি গবেষণা ও প্রশিক্ষণ ইনস্টিটিউট (বারটান), সেচ ভবন, মানিকমিয়া এভিনিউ, ঢাকা।
১৫) নির্বাহী পরিচালক, বরেন্দ্র বহুমুখী উন্নয়ন কর্তৃপক্ষ, রাজশাহী।
১৬) নির্বাহী পরিচালক, তুলা উন্নয়ন বোর্ড, খামারবাড়ি, ঢাকা।
১৭) পরিচালক, বীজ প্রত্যয়ন এজেন্সী, জয়দেবপুর, গাজীপুর।
১৮) পরিচালক, কৃষি তথ্য সার্ভিস, খামারবাড়ি, ফার্মগেট, ঢাকা।

অনুলিপি:

১। অতিরিক্ত সচিব (পিপিসি) মহোদয়ের ব্যক্তিগত কর্মকর্তা, কৃষি মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা।
২। অতিরিক্ত সচিব (পিপিবি) মহোদয়ের ব্যক্তিগত কর্মকর্তা, কৃষি মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা।
৩। অফিস কপি।

কৃষিই সমৃদ্ধি

অতি জরুরি
ই-মেইল মারফত

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
কৃষি মন্ত্রণালয়
নীতি-১ শাখা
www.moa.gov.bd

স্মারক নং-১২.০০.০০০০.০৭৫.২২.০৪৭.১৯. ১৩৮

তারিখ : ২৭/০৭/১৪২৬ ব:
১২/১১/২০১৯ খ্রি:

বিষয়: 'ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা'-এর খসড়ার ওপর মতামত প্রেরণ।

সূত্র: মন্ত্রিপরিষদ বিভাগ (ই-গভর্নেন্স-১ অধিশাখা) এর স্মারক নম্বর: ০৪.০০.০০০০.৮৩১.২২.০০৩.১৯.৫৮; তারিখ: ৩০ অক্টোবর ২০১৯

উপর্যুক্ত বিষয়ের প্রেক্ষিতে জানানো যাচ্ছে যে, মন্ত্রিপরিষদ বিভাগ কর্তৃক প্রেরিত পত্রের অনুলিপি এতদসঙ্গে প্রেরণ করা হলো। সকল সরকারি কার্যালয়ে ব্যবহারের জন্য সমন্বিত ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা, ২০১৯-এর খসড়া প্রণয়ন করা হয়েছে। আগামী ২০ নভেম্বর ২০১৯ তারিখের মধ্যে উক্ত খসড়া নির্দেশিকার ওপর মতামত প্রেরণের জন্য অনুরোধ করা হয়েছে।

০২। বর্ণিতাবস্থায়, উক্ত বিষয়ের উপর আগামী ০৩ কর্ম দিবসের মধ্যে মতামত প্রদানের জন্য নির্দেশক্রমে অনুরোধ করা হলো।

সংযুক্তি: বর্ণনামতে।

(মোঃ হানিফ উদ্দিন)
উপসচিব
ফোন: ৯৫৪০৩৮৫
ই-মেইল: moapolicy1@gmail.com

বিতরণ (জ্যেষ্ঠতার ভিত্তিতে নয়) :

১) নির্বাহী চেয়ারম্যান, বাংলাদেশ কৃষি গবেষণা কাউন্সিল, ফার্মগেট, ঢাকা।
২) চেয়ারম্যান, বাংলাদেশ কৃষি উন্নয়ন কর্পোরেশন, কৃষি ভবন, ৪৯-৫১ মতিঝিল বা/এ, ঢাকা।
৩) মহাপরিচালক, কৃষি বিপণন অধিদপ্তর, খামারবাড়ি, ঢাকা।
৪) মহাপরিচালক, কৃষি সম্প্রসারণ অধিদপ্তর, খামারবাড়ি, ঢাকা।
৫) মহাপরিচালক, বাংলাদেশ ধান গবেষণা ইনস্টিটিউট, জয়দেবপুর, গাজীপুর।
৬) মহাপরিচালক, বাংলাদেশ পাট গবেষণা ইনস্টিটিউট, মানিক মিয়া এভিনিউ, ঢাকা।
৭) মহাপরিচালক, জাতীয় কৃষি প্রশিক্ষণ একাডেমি (নাটা), গাজীপুর।
৮) মহাপরিচালক, বাংলাদেশ কৃষি গবেষণা ইনস্টিটিউট, জয়দেবপুর, গাজীপুর।
৯) মহাপরিচালক, বাংলাদেশ সুগারক্রপ গবেষণা ইনস্টিটিউট, ঈশ্বরদী, পাবনা।
১০) মহাপরিচালক, বাংলাদেশ পরমানু কৃষি গবেষণা ইনস্টিটিউট (বিনা), ময়মনসিংহ।
১১) মহাপরিচালক, বাংলাদেশ গম ও ভুট্টা গবেষণা ইনস্টিটিউট, নশিপুর, দিনাজপুর।
১২) ব্যবস্থাপনা পরিচালক, হর্টেক্স ফাউন্ডেশন, সেচ ভবন (৩য় তলা), মানিক মিয়া এভিনিউ, ঢাকা।
১৩) পরিচালক, মৃত্তিকা সম্পদ উন্নয়ন ইনস্টিটিউট, মৃত্তিকা ভবন, ফার্মগেট, ঢাকা।
১৪) নির্বাহী পরিচালক, বাংলাদেশ ফলিত পুষ্টি গবেষণা ও প্রশিক্ষণ ইনস্টিটিউট (বারটান), সেচ ভবন, মানিকমিয়া এভিনিউ, ঢাকা।
১৫) নির্বাহী পরিচালক, বরেন্দ্র বহুমুখী উন্নয়ন কর্তৃপক্ষ, রাজশাহী।
১৬) নির্বাহী পরিচালক, তুলা উন্নয়ন বোর্ড, খামারবাড়ি, ঢাকা।
১৭) পরিচালক, বীজ প্রত্যয়ন এজেন্সী, জয়দেবপুর, গাজীপুর।
১৮) পরিচালক, কৃষি তথ্য সার্ভিস, খামারবাড়ি, ফার্মগেট, ঢাকা।

অনুলিপি:

১। অতিরিক্ত সচিব (পিপিসি) মহোদয়ের ব্যক্তিগত কর্মকর্তা, কৃষি মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা।
২। অতিরিক্ত সচিব (পিপিবি) মহোদয়ের ব্যক্তিগত কর্মকর্তা, কৃষি মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা।
৩। অফিস কপি।

খসড়া

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

২০১৯ 'ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা ,ডিজিটাল ডিভাইস'

মন্ত্রিপরিষদ বিভাগ

১. প্রেক্ষাপট :

বাংলাদেশকে ২০২১ সালের মধ্যে মধ্যম আয়ের দেশ এবং ২০৪১ সালের মধ্যে উন্নত দেশে উন্নীত করতে সরকার ব্যাপক উন্নয়ন কার্যক্রম গ্রহণ করেছে। সরকারের বহুমুখী এ সকল উন্নয়ন কার্যক্রম দ্রুত এবং সফল বাস্তবায়নের পাশাপাশি জনগণের দোরগোড়ায় দ্রুত ও মানসম্মত সেবা প্রদানের লক্ষ্যে তথ্য ও যোগাযোগ প্রযুক্তি ব্যবহার ব্যাপকভাবে বৃদ্ধি পাচ্ছে। তথ্য ও যোগাযোগ প্রযুক্তি ব্যবহার বৃদ্ধির সঙ্গে সঙ্গে কম্পিউটার ও ইন্টারনেটে রক্ষিত ব্যক্তিগত ও গুরুত্বপূর্ণ তথ্যসমূহের নিরাপত্তার ঝুঁকিও বৃদ্ধি পেয়েছে। তথ্য সুরক্ষা বিষয়ক সক্ষমতার অভাব, বিশেষায়িত জ্ঞান ও দক্ষ জনবলের অভাবসহ নানাবিধ কারণে বিভিন্ন প্রতিষ্ঠান সাইবার আক্রমণের শিকার হচ্ছে। এ সব আক্রমণ হতে ডিজিটাইজড তথ্য সম্পদ সুরক্ষায় পর্যাপ্ত নিরাপত্তামূলক ব্যবস্থা গ্রহণ করা প্রয়োজন। এ লক্ষ্যে সকল সরকারি প্রতিষ্ঠানের ডিজিটাল ডিভাইস ও তথ্য সুষ্ঠুভাবে সংরক্ষণসহ নিরাপত্তা ব্যবস্থা গ্রহণের জন্য -ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা ,ডিজিটাল ডিভাইস' '২০১৯ প্রণয়ন করা হল। এ নির্দেশিকা অনুসরণের মাধ্যমে ডিজিটাল তথ্য ব্যবস্থার সঙ্গে সংশ্লিষ্ট কর্মকর্তা-কর্মচারীগণ তথ্যের নিরাপত্তায় অধিকতর দায়িত্বশীল ভূমিকা পালন করতে সক্ষম হবেন।

২. সংজ্ঞা: বিষয় বা প্রসঙ্গের পরিপন্থী কোনো কিছু না থাকলে, এই নির্দেশিকায়-

(১) "ডিজিটাল তথ্য" অর্থ টেক্সট, ইমেজ, অডিও বা ভিডিও আকারে প্রস্তুত তথ্য, জ্ঞান, ঘটনা, ধারণা বা নির্দেশাবলী যা কম্পিউটার প্রিন্ট আউট, ম্যাগনেটিক বা অপটিক্যাল স্টোরেজ মিডিয়া, পাঞ্চকার্ড, পাঞ্চ টেপসহ যে কোন আকারে বা বিন্যাসে কম্পিউটার সিস্টেম অথবা কম্পিউটার নেটওয়ার্কে প্রক্রিয়াজাত করা হয়েছে, হচ্ছে বা হবে অথবা অভ্যন্তরীণভাবে যা কোন কম্পিউটার স্মৃতিতে সংরক্ষিত;

(২) "ডিজিটাল ডিভাইস" অর্থ কোনো ইলেকট্রনিক, ডিজিটাল, ম্যাগনেটিক, অপটিক্যাল বা তথ্য প্রক্রিয়াকরণ যন্ত্র বা সিস্টেম যা ইলেট্রনিক, ডিজিটাল, ম্যাগনেটিক বা অপটিক্যাল ইমপালস ব্যবহার করে যৌক্তিক, গাণিতিক এবং স্মৃতি বিষয়ক কার্যক্রম সম্পন্ন করে অথবা কোন ডিজিটাল সিস্টেম বা নেটওয়ার্কের সঙ্গে সংযুক্ত হয়ে সকল ইনপুট, আউটপুট, প্রক্রিয়াকরণ, সঞ্চিত, যোগাযোগ ইত্যাদি কার্যক্রম সম্পন্ন করে তা এর অন্তর্ভুক্ত হবে;

(৩) "তথ্য" অর্থ এ নির্দেশিকার অনুচ্ছেদ-২ (১) এ বর্ণিত ডিজিটাল তথ্য;

(৪) "তথ্য নিরাপত্তা নিরীক্ষা" অর্থ তথ্য যথাযথভাবে সংরক্ষণ করা হয়েছে কি না তা পর্যবেক্ষণ এবং মূল্যায়ন;

(৫) "ভাইরাস" অর্থ এক ধরনের কম্পিউটার প্রোগ্রাম বা কোড বা নির্দেশনা যা কোন কম্পিউটার বা ডিজিটাল ডিভাইসে সংক্রমণের ফলে স্বয়ংক্রীয়ভাবে তথ্য পরিবর্তন, বিনাশ, ক্ষতি বা এর কার্যসম্পাদনের দক্ষতায় বিরূপ প্রভাব বিস্তার করে;

(৬) 'ম্যালওয়ার 'অর্থ এমন কোনো কম্পিউটার বা ডিজিটাল নির্দেশ, তথ্য-উপাত্ত, প্রোগ্রাম বা এ্যাপস যা -

(ক) কোনো কম্পিউটার বা ডিজিটাল ডিভাইস কর্তৃক সম্পাদিত কার্যকে পরিবর্তন, বিকৃত, বিনাশ, ক্ষতি বা ক্ষুন্ন করে বা এর কার্য সম্পাদনে বিরূপ প্রভাব বিস্তার করে;

(খ) নিজেকে অন্য কোনো কম্পিউটার বা ডিজিটাল ডিভাইসের সাথে সংযুক্ত করে উক্ত কম্পিউটার বা ডিজিটাল ডিভাইসের কোনো প্রোগ্রাম, তথ্য-উপাত্ত বা নির্দেশ কার্যকর করার বা কোনো কার্য সম্পাদনের সময় স্বপ্রণোদিতভাবে ক্রিয়াশীল হয়ে উঠে এবং উক্ত কম্পিউটার বা ডিজিটাল ডিভাইসে কোনো ক্ষতিকর পরিবর্তন বা ঘটনা ঘটায়;

(গ) কোনো ডিজিটাল ডিভাইসের তথ্য চুরি বা তাতে স্বয়ংক্রিয় প্রবেশের সুযোগ সৃষ্টি করে।

(৭)'সাইবার ঘটনাঅর্থ সাইবার নিরাপত্তা সংক্রান্ত বৈরী পরি 'স্থিতিকে বুঝাবে যেখানে নিরাপত্তা ব্যবস্থা ও নীতিমালা ভঙ্গ করে অনুনমোদিত প্রবেশ সংগঠিত হয়। কোনো সেবা প্রদান বন্ধ বা ব্যাহত হয় এবং কম্পিউটার

ও কম্পিউটার সিস্টেম অনুনমোদিত ব্যবহারের মাধ্যমে তথ্য পরিবর্তনউপাত্ত প্রক্রিয়াকরণ ও সংগৃহীত -তথ্য , হয়।

(৮) "সামাজিক যোগাযোগ মাধ্যম" অর্থ কম্পিউটার বা ডিজিটাল ডিভাইসে ইন্টারনেট ব্যবহারের মাধ্যমে পারস্পরিক যোগাযোগের উদ্দেশ্যে তথ্য-উপাত্ত (টেক্সট, ইমেজ, অডিও, ভিডিও ইত্যাদি) আদান-প্রদানের একটি প্ল্যাটফরম;

(৯) "সরকারি প্রতিষ্ঠান" অর্থ কোন আইন, বিধি বা সরকারি আদেশ বলে প্রতিষ্ঠিত প্রতিষ্ঠান, সংবিধিবদ্ধ সংস্থা, অথবা সরকারের মালিকানা বা নিয়ন্ত্রণাধীন কোনো প্রতিষ্ঠান বা কর্তৃপক্ষ;

৩. উদ্দেশ্য:

(১) ডিজিটাল তথ্য সম্পর্কে ধারণা, সংরক্ষণ এবং নিরাপত্তা বিষয়ে প্রাতিষ্ঠানিক সক্ষমতা ও সচেতনতা বৃদ্ধি করা;

(২) ডিজিটাল ডিভাইস, সফটওয়্যার ও নেটওয়ার্ক যথাযথভাবে সংরক্ষণ ও নিরাপদ রাখা;

(৩) ইন্টারনেট, ওয়েবসাইট ও সামাজিক যোগাযোগ মাধ্যম ব্যবহারে সচেতনতা বৃদ্ধি করা।

৪. নির্দেশিকার পরিধি:

সকল সরকারি প্রতিষ্ঠানের ডিজিটাল তথ্যের নিরাপত্তা নিশ্চিত করার জন্য এ নির্দেশিকা প্রণয়ন করা হয়েছে। ডিজিটাল তথ্যের সুরক্ষা বিষয়ে সরকারি বিভিন্ন আইন, বিধিমালা, প্রজ্ঞাপন, পরিপত্র, নির্দেশনা ইত্যাদির সহায়ক দলিল হিসেবে এ নির্দেশিকা ব্যবহৃত হবে। সকল সরকারি প্রতিষ্ঠানসমূহ এ নির্দেশিকা অনুসরণ করবে।

৫. ডিজিটাল ডিভাইস ও তথ্য ব্যবস্থাপনা:

৫.১. ইনভেন্টরি তৈরি:

সুষ্ঠু তথ্য ব্যবস্থাপনার জন্য প্রতিষ্ঠানের ডিজিটাল ডিভাইস এবং তথ্যের ইনভেন্টরি প্রস্তুত করা প্রয়োজন। ইনভেন্টরি প্রস্তুত করার সময় সকল সম্পদের গুরুত্ব বিবেচনায় এনে তালিকাভূক্ত করতে হবে। ইনভেন্টরিতে সম্পদের ধরন, আকার, অবস্থান, ব্যাকআপ, লাইসেন্স বিষয়ক তথ্য, প্রতিষ্ঠানের কাছে এর প্রয়োজনীয়তা এবং মূল্যসহ অন্যান্য প্রয়োজনীয় সকল তথ্য অন্তর্ভুক্ত রাখতে হবে।

৫.২. তথ্য শ্রেণিকরণ:

তথ্য যথাযথভাবে সংরক্ষণ এবং তথ্যভান্ডারে অনধিকার প্রবেশ রোধে তথ্যের শ্রেণিকরণ করা প্রয়োজন। তথ্যের শ্রেণিকরণের ক্ষেত্রে তথ্যের গোপনীয়তা, প্রয়োজনীয়তা, অগ্রাধিকার ও তথ্য ব্যবহারে প্রত্যাশিত সুরক্ষা প্রদানের বিষয় বিবেচনা করতে হবে। বিভিন্ন প্রতিষ্ঠানের তথ্যের স্পর্শকাতরতা ও গুরুত্বের ভিন্ন ভিন্ন মাত্রা রয়েছে। কিছু কিছু তথ্য অধিকমাত্রায় সুরক্ষা বা নিয়ন্ত্রণ করা প্রয়োজন হতে পারে। সে জন্য সরকারি বিধি-বিধানের আলোকে তথ্যের নিরাপত্তাস্তর নির্ধারণসহ তথ্য যথাযথভাবে সংরক্ষণে শ্রেণিকরণ করতে হবে।

৫.৩. তথ্য নিরাপত্তার কৌশলসমূহ:

(ক) তথ্য নিরাপত্তা কৌশল প্রণয়নের নিমিত্ত জনবল ও প্রযুক্তির সমন্বয়ে কর্ম-পরিকল্পনা গ্রহণ করতে হবে।

(খ) তথ্য নিরাপত্তা সম্পর্কিত নতুন নতুন হুমকি/ঝুঁকি নিরসনের লক্ষ্যে নিয়মিত প্রতিষ্ঠানের গৃহীত কৌশলসমূহ পরীক্ষা করে দেখতে হবে। তথ্য নিরাপত্তা কৌশলের বিভিন্ন পদ্ধতিসমূহ সম্পর্কে ধারণা নিয়ে প্রতিষ্ঠানের প্রয়োজন অনুযায়ী অনুশীলনযোগ্য টেকসই পদ্ধতির নিরাপত্তা কৌশল প্রণয়ন করতে হবে।

(গ) তথ্য নিরাপত্তা নিয়ন্ত্রণে যন্ত্রপাতির নিয়ন্ত্রণ, প্রবেশাধিকার নিয়ন্ত্রণ, ভৌত ও পরিবেশগত নিরাপত্তা ব্যবস্থা, সফটওয়্যারের নিরাপত্তা ও ব্যাক-আপ ব্যবস্থা, নেটওয়ার্ক নিরাপত্তা-ব্যবস্থাপনা, ক্রিপ্টোগ্রাফিক নিয়ন্ত্রণ, প্রক্রিয়াকরণ ইত্যাদি বিষয়সমূহ গুরুত্বের সঙ্গে বিবেচনা করতে হবে।

(ঘ) হার্ডওয়্যার, সফটওয়্যার, নেটওয়ার্ক ইত্যাদি সেবা গ্রহণ কার্যক্রমে ব্যবহারের Service Level Agreement রয়েছে কি না নিশ্চিত হতে হবে।

৫.৪. ডিজিটাল ডিভাইস সুরক্ষায় করণীয়:

(ক) কম্পিউটারের সঙ্গে ইউপিএস ব্যবহার করা;

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

(গ) ডেস্ক থেকে উঠে যাবার সময় ব্যবহৃত কম্পিউটার/ল্যাপটপ সিস্টেম লক করে যাওয়া;

(ঘ) কম্পিউটার/ল্যাপটপ সংরক্ষিত গুরুত্বপূর্ণ ফাইলসমূহ zip করে ব্যকআপ রাখা;

(ঙ) কম্পিউটার/ল্যাপটপে ইউএসবি পোর্টের ব্যবহার নিয়ন্ত্রণ করা;

(চ) কম্পিউটার/ল্যাপটপ/মোবাইল-এ লাইসেন্স-ভার্সন এন্টিভাইরাস সফটওয়্যার ব্যবহার করা এবং নিয়মিত আপডেট রাখা;

(ছ) সংশ্লিষ্ট ডিজিটাল ডিভাইসে Biometric Authentication (Finger Print, Scans Option ইত্যাদি) থাকলে তা Enable রাখা;

(জ) কম্পিউটার/ল্যাপটপ/মোবাইলে অপ্রয়োজনীয় Service বন্ধ রাখা;

(ঝ) ডেস্কটপ/ল্যাপটপ/মোবাইল/ট্যাবে অননুমোদিত সফটওয়্যার ইনস্টল না করা;

(ঞ) ডেস্কটপ/ল্যাপট/মোবাইল/ট্যাব অপরিচিত কোন ব্যক্তিকে ব্যবহার করতে না দেয়া;

(ট) পেনড্রাইভ, এক্সটার্নাল হার্ডডিস্ক, মেমরি কার্ড, সিডি/ডিভিডি ডিস্ক ইত্যাদি ভাইরাস স্ক্যান করে ব্যবহার করা;

(ঠ) গুরুত্বপূর্ণ ডকুমেন্টসমূহ পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;

(ড) লাইসেন্সকৃত আপডেটেড অপারেটিং সিস্টেম, এন্টিভাইরাস, এপ্লিকেশন সফটওয়্যার ইত্যাদি ব্যবহার করা;

(ড) অপারেটিং সিস্টেমে ফায়ারওয়াল চালু রাখা;

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

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

(থ) তথ্য-উপাত্ত নিয়মিত বিকল্প স্টোরেজ ডিভাইস এ ব্যাক-আপ রাখা;

(দ) নিরাপত্তার বিষয়ে নিশ্চিত না হয়ে ফ্রি সফটওয়্যার ডাউনলোড করা থেকে বিরত থাকা;

(ধ) নিয়মিত ডিজিটাল ডিভাইস পরিষ্কার পরিচ্ছন্ন রাখা ;

(ন) হার্ডওয়্যারের কোয়ালিটি টেস্ট নিশ্চিত করা;

(প (কম্পিউটার/ল্যাপটপ/ট্যাবের physical security নিশ্চিত করা;

(ফ) কম্পিউটার/ল্যাপটপ/ট্যাবের কাজ শেষ হওয়া মাত্র shut down কমান্ড দিয়ে বন্ধ করা।

৫.৫. সফট্ওয়্যারের নিরাপত্তায় করণীয়:

(ক) সফট্ওয়্যার প্রস্তুতের সময় সংশ্লিষ্ট বাংলাদেশ ন্যাশনাল ডিজিটাল আর্কিটেকচার ফ্রেমওয়ার্ক (BNDA) যথাযথভাবে অনুসরণ করা;

(খ) বাংলাদেশ কম্পিউটার কাউন্সিল কর্তৃক সফটওয়্যারের কোয়ালিটি টেস্ট নিশ্চিত করে ব্যবহার করা;

(গ) সফটওয়্যারে ইউজার পাসওয়ার্ড এনক্রিপ্ট করে রাখা;

(ঘ) ওয়েব এপ্লিকেশন নিরাপত্তার জন্য SSL সার্টিফিকেশন ব্যবহার করা;

(ঙ) সফটওয়্যারের Vulnerability নিয়মিত পরীক্ষা করা এবং প্রাপ্ত ফলাফলের ভিত্তিতে প্রয়োজনীয় পদক্ষেপ নেয়া;

(চ) সফটওয়্যার বা ওয়েবসাইটে অ্যাডমিন ইউজারের পাসওয়ার্ড নিয়মিত পরিবর্তনের অপশন রাখা;

(ছ) সফটওয়্যার বা ওয়েবসাইটের লগইন পাতায় অধিক নিরাপত্তার জন্য 2-Factor Authentication ব্যবস্থা রাখা;

(জ) লগ-ইন এলার্ট ব্যবহার করা;

(ঝ) প্রস্তুতকৃত সফটওয়্যারের সোর্সকোড, ডাটাবেইজ এবং ডকুমেন্টেশন সংরক্ষণ নিশ্চিত করা; এবং

(ঞ) সফটওয়্যারের চুক্তির মেয়াদ শেষ হওয়ার পূর্বেই যথাসময়ে প্রয়োজনীয় ব্যবস্থা গ্রহণ করা;

৫.৬. 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) পাসওয়ার্ড তৈরি ও রিকভারি করার সময় সিকিউরিটি চেকের ব্যবস্থা রাখা;

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

(ঘ) পাসওয়ার্ড তৈরিতে নিজের নাম, জন্ম তারিখ, ব্যাংক অ্যাকাউন্ট নম্বর, স্ত্রী অথবা সন্তানের নাম ও জন্ম তারিখ, বিবাহ বার্ষিকীর তারিখ ইত্যাদি সচরাচর ব্যবহৃত বিষয়সমূহ ব্যবহারে বিরত থাকা;

(ঙ) নিয়মিত (অন্তত ২/৩ মাস পর পর) পাসওয়ার্ড পরিবর্তন করা এবং

(চ) পাসওয়ার্ড পরিবর্তনের সময় সিস্টেমে স্বয়ংক্রিয় সতর্কবার্তা প্রদর্শন করার ব্যবস্থা রাখা।

৫.৭. লোকাল এরিয়া নেটওয়ার্ক (LAN) সুরক্ষায় করণীয়:

(ক) LAN-এ অননুমোদিত ব্যক্তির ডিজিটাল ডিভাইস ব্যবহার নিয়ন্ত্রণ করা;

(খ) নেটওয়ার্ক সুরক্ষার জন্য ম্যানেজেবল সুইচ, ফায়ারওয়্যাল, রাউটার ইত্যাদি ব্যবহার করা;

(গ) ডিজিটাল ডিভাইসে রিমোট অ্যাকসেসের বিষয়ে সতর্ক থাকা;

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

(ঙ) সিস্টেম বা নেটওয়ার্কে বিদ্যমান নিরাপত্তা ব্যবস্থার কার্যকারিতা যাচাইয়ের জন্য নিয়মিত পরীক্ষা করা;

(চ) নিয়মিত নেটওয়ার্ক মনিটরিং সিস্টেম মনিটর করা;

(ছ) সার্ভারসহ অন্যান্য গুরত্বপূর্ণ এ্যাপ্লিকেশনসমূহ ল্যান ব্যবস্থাপনা থেকে পৃথক নিরাপত্তা ব্যবস্থাপনায় রাখা;

৫.৮. ইন্টারনেট ব্যবস্থাপনায় করণীয়:

(ক) সরকার অনুমোদিত আইএসপি প্রতিষ্ঠান হতে ইন্টারনেটের সংযোগ নেওয়া;

(খ) যথাযথ ব্যবস্থাপনার মাধ্যমে ইন্টারনেট ব্যান্ডউইথের সর্বোচ্চ ব্যবহার নিশ্চিত করা;

(গ) ইন্টারনেট সংযোগের ক্ষেত্রে অনুমোদিত ডিভাইস ব্যবহার নিশ্চিত করা;

(ঘ) ব্রাউজারে পাসওয়ার্ড স্থায়ীভাবে সংরক্ষণ না করা;

(ঙ) নিয়মিত ব্রাউজার আপডেট রাখা;

(চ) ফ্রি প্রক্সি সাইট ব্যবহার থেকে বিরত থাকা;

(ছ) পাবলিক হটস্পট থেকে অনলাইন অ্যাকাউন্ট ব্যবহারের সময় সতর্কতা অবলম্বন করা;

(জ) ওয়াই-ফাই রাউটার পাসওয়ার্ড নিয়মিত পরিবর্তন করা;

(ঝ) প্রসিদ্ধ ওয়েবসাইট ছাড়া অন্য সোর্স থেকে ফ্রি সফটওয়্যার ডাউনলোড করা থেকে বিরত থাকা।

৫.৯. ই-মেইল ব্যবস্থাপনায় করণীয়:

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

(খ) ই-মেইল সিকিউরিটি গেটওয়ে ব্যবহার নিশ্চিত করা;

(গ) নিয়মিত ই-মেইলের পাসওয়ার্ড পরিবর্তন করা;

(ঘ) ই-মেইলে ব্যবহৃত পাসওয়ার্ড অন্য কারো সঙ্গে শেয়ার না করা;

(ঙ) ই-মেইলের পাসওয়ার্ড কোথাও লিখে না রাখা;

(চ) ই-মেইল ব্যবহার শেষে লগ আউট হওয়া;

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

(জ) সন্দেহজনক ই-মেইল বা সংযুক্তি না খোলা;

(ঝ) ই-মেইল থেকে নিয়মিত অপ্রয়োজনীয় তথ্যাদি অপসারণ করা এবং

(ঞ) খুব বেশী জরুরি না হলে অন্যের কম্পিউটার থেকে ই-মেইল, সোস্যাল মিডিয়া প্ল্যাটফরম ইত্যাদিতে লগইন করা থেকে বিরত থাকা;

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

(ঠ) অন্যের কম্পিউটারে ইমেইল, সোস্যাল মিডিয়া বা অন্য কোনো সাইটে লগইন করার ক্ষেত্রে ব্রাউজারে "Incognito" মোড বা প্রাইভেট মোড ব্যবহার করা; এবং

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

৫.১০. সার্ভারকক্ষ সুরক্ষায় করণীয়:

(ক) সার্ভারকক্ষে প্রবেশে কঠোর নিয়ন্ত্রণ ব্যবস্থা বজায় রাখা;

(খ) প্রয়োজনে নিরাপত্তাকর্মীর মাধ্যমে সার্ভারকক্ষের সার্বক্ষণিক নিরাপত্তা নিশ্চিত করা;

(গ) সার্ভারকক্ষের দরজায় উন্নতমানের লকের ব্যবস্থা রাখা;

(ঘ) সার্বক্ষণিক সিসিটিভি'র মাধ্যমে নজরদারির ব্যবস্থা রাখা;

(ঙ) ভিজিটর অথবা ভেন্ডরদের সার্ভারকক্ষে প্রবেশের তথ্য রেজিস্টারে লিপিবদ্ধ রাখা;

(চ) ফিঙ্গারপ্রিন্টসহ অন্যান্য বায়োমেট্রিক সিকিউরিটি সিস্টেমের ব্যবস্থা রাখা;

(ছ) সার্ভার কক্ষে নিরবচ্ছিন্ন বিদ্যুৎ সরবরাহ ও শীতাতপ নিয়ন্ত্রণের ব্যবস্থা রাখা; এবং

(জ) স্বয়ংক্রিয় অগ্নিনির্বাপন সিস্টেমের ব্যবস্থা রাখা।

৫.১১. সার্ভার সুরক্ষায় করণীয়:

(ক) সার্ভারের সঙ্গে অনলাইন ইউপিএস-এর ব্যবহার নিশ্চিত করা;

(খ) সার্ভার অবশ্যই পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;

(গ) সার্ভারে ইউএসবি পোর্টের ব্যবহার নিয়ন্ত্রণ করা;

(ঘ) সার্ভার-কে ভাইরাস, স্পাইওয়্যার, মালওয়্যার, অ্যাডওয়্যার এবং অন্যান্য আক্রমণ মুক্ত রাখার জন্য লাইসেন্স-ভার্সন এন্টিভাইরাস সফটওয়্যার ব্যবহার করা, এন্টি-স্পাইওয়্যার ব্যবহার করা, সফটওয়্যার প্যাচ আপডেট রাখা এবং ফায়ারওয়াল চালু রাখা;

(ঙ) সার্ভারে Biometric Authentication like Finger Print, Scans Option থাকলে তা Enable করে রাখা;

(চ) সার্ভারের অপ্রয়োজনীয় Service বন্ধ রাখা;

(ছ) সার্ভারে অননুমোদিত সফটওয়্যার ইনস্টল না করা;

(জ) পেনড্রাইভ, মোবাইল হার্ডডিস্ক, মেমরি কার্ড, সিডি/ডিভিডি ডিস্ক ইত্যাদি ভাইরাস স্ক্যান করে ব্যবহার করা;

(ঝ) লাইসেন্সকৃত আপডেটেড অপারেটিং সিস্টেম, এন্টিভাইরাস, এপ্লিকেশন সফটওয়্যার ইত্যাদি ব্যবহার করা;

(ঞ) ব্লু-টুথ, ওয়াই-ফাই, ইনফ্রারেড ইত্যাদি বন্ধ রাখা;

(ট) ডাটাবেইজের নিয়মিত ব্যাক-আপ নিশ্চিত করা;;

(ঠ) সার্ভারে লগ ফাইল নিয়মিত পর্যবেক্ষণ করা;

(ড) অডিট লগ চালু রাখা;

(ঢ) যে কোন চলমান সিস্টেমের ব্যাকআপ সার্ভার প্রস্তুত রাখা;

(ণ) নিরাপত্তার বিষয়ে নিশ্চিত না হয়ে ফ্রি সফটওয়্যার ডাউনলোড করা থেকে বিরত থাকা;

(ত) নিয়মিত সার্ভারকে পরিষ্কার পরিচ্ছন্ন রাখা;

(থ (সার্ভারের physical security নিশ্চিত করা;

(দ) প্রয়োজনে বাংলাদেশ কম্পিউটার কাউন্সিল কর্তৃক সার্ভারের হার্ডওয়্যারের কোয়ালিটি টেস্ট করা;

৫.১২. সামাজিক যোগাযোগ মাধ্যম সুরক্ষায় করণীয়:

(ক) সামাজিক যোগাযোগ মাধ্যম ব্যবহারের সময় সংশ্লিষ্ট ব্যক্তিবর্গের প্রোফাইল সম্পর্কে জানা ও সচেতন থাকা;

(খ) সামাজিক যোগাযোগ মাধ্যম যেমন: ফেসবুক, টুইটার, স্কাইপি, ইমো, ভাইবার, হোয়াটসঅ্যাপ ইত্যাদিতে কোন পোস্ট/আপলোড, কমেন্ট, লাইক, বন্ধু বাছাই, শেয়ার করার ক্ষেত্রে যথাযথ সতর্কতা অবলম্বন করা;

(গ) অসামাজিক কোন সাইটে (যেমন: পর্নোসাইট, জুয়া বা লটারি বিষয়ক সাইট, জঙ্গিবাদ বিষয়ক সাইট ইত্যাদি) প্রবেশ থেকে বিরত থাকা;

(ঘ) সামাজিক যোগাযোগ মাধ্যম ব্যবহারের ক্ষেত্রে সেটিংস থেকে লগইন নোটিফিকেশন অপশন চালু রাখা;

(ঙ) নিজের অ্যাকাউন্টে অতিরিক্ত আরেকটি ই-মেইল ঠিকানা বা মোবাইল নম্বর যোগ করা যাতে কোনোভাবে অ্যাকাউন্ট হ্যাক হলে পুনরুদ্ধার করা যায়;

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

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

৬. ঝুঁকি ব্যবস্থাপনা:

৬.১ ঝুঁকি বিশ্লেষণ:

ডিজিটাল তথ্যসম্পদের ঝুঁকি বিশ্লেষণ অত্যন্ত গুরুত্বপূর্ণ। **এ ক্ষেত্রে** ঝুঁকির ক্ষেত্রসমূহ শনাক্ত করার পাশাপাশি তথ্যসম্পদ সুরক্ষার ক্ষেত্রে যে সকল সমস্যা/প্রতিবন্ধকতা থাকতে পারে তা যথাযথ বিশ্লেষণ করে প্রতিকারের উপায় চিহ্নিত করতে হবে। প্রতিষ্ঠানের কোথায়, কখন, কীভাবে কোন প্রকৃতির **আকস্মিক ঘটনা** ঘটতে পারে তা যথাযথভাবে বিশ্লেষণ করা দরকার যাতে তথ্যসম্পদে যে সকল **আকস্মিক ঘটনা** ঘটার সম্ভাবনা আছে বা ভবিষ্যতে ঘটতে পারে তার প্রতিটি বিষয় পুঙ্খানুপুঙ্খ শনাক্ত করে সে অনুযায়ী প্রয়োজনীয় পদক্ষেপ গ্রহণ করা যায়।

৬.২ ঝুঁকি মোকাবেলায় কর্মপরিকল্পনা প্রণয়ন:

ঝুঁকি প্রশমন করার জন্য ঝুঁকি বিশ্লেষণ অত্যন্ত গুরুত্বপূর্ণ। ঝুঁকি বিশ্লেষণের ফলাফলের ওপর ভিত্তি করে ঝুঁকিসমূহকে কিভাবে প্রশমন করা যায় সে বিষয়ে সিদ্ধান্ত গ্রহণ করার জন্য ঝুঁকির ফলাফল ও ঝুঁকির মাত্রা বিবেচনা করে একটি সার্বিক কর্ম-পরিকল্পনা প্রণয়ন করতে হবে। এ কর্মপরিকল্পনায় বিভিন্ন পর্যায়ে থাকতে পারে। যেমন:

ক. ঘটনা ঘটার পূর্বে, প্রতিরোধমূলক ব্যবস্থার মাধ্যমে ঝুঁকি অপসারণ;

খ. ঘটনা ঘটার সময়, ঝুঁকি শনাক্তকরণের মাধ্যমে ঝুঁকি অপসারণ;

গ. ঘটনা ঘটার পর, সংশোধনমূলক ব্যবস্থা গ্রহণ করে ঝুঁকি অপসারণ।

৬.৩ আকস্মিক ঘটনা ব্যবস্থাপনা:

তথ্য নিরাপত্তায় দূর্ঘটনা যে কোনো সময় ঘটতে পারে । এ বিষয়টি বিবেচনায় নিয়ে যথাযথ সতর্কতা অবলম্বন করা প্রয়োজন যাতে যে কোনো ধরনের আকস্মিক দুর্যোগ যেমন-বন্যা, অগ্নিকান্ড, ভূমিকম্প ইত্যাদির সময় দাপ্তরিক কার্যক্রমের ধারাবাহিকতা রক্ষায় স্বল্প সময়ের মধ্যে তথ্য ব্যবস্থা পুনরুদ্ধার কার্যক্রম শুরু করা যায়। **আকস্মিক ঘটনা মোকাবিলার জন্য সকল প্রতিষ্ঠানের একটি জরুরি সাড়া প্রদানকারী টিম গঠন করা প্রয়োজন। অনেক ক্ষেত্রে এ ধরনের পরিস্থিতি শুধুমাত্র প্রতিষ্ঠানের নিজস্ব জনবল দ্বারা মোকাবিলা করা সম্ভব হয় না। এ কারণে জুরুরি সাড়া প্রদানকারী টিম গঠনের ক্ষেত্রে নিজস্ব জনবলের পাশাপাশি অন্যান্য বিশেষায়িত প্রতিষ্ঠানের সদস্যগণকেও অন্তর্ভুক্ত করা যেতে পারে। আকস্মিক ঘটনা মোকাবিলার জন্য এ টিমের কর্ম-পরিকল্পনা থাকতে হবে।** বিশেষজ্ঞটিম ঘটনা ঘটার পরপরই তদন্তপূর্বক যথাযথ রিপোর্ট প্রদান করবে। **আকস্মিক ঘটনা** তদন্তের পর সংশ্লিষ্ট রেকর্ডসমূহ যথাযথভাবে সংরক্ষণ করতে হবে। অধিকন্তু এ রিপোর্ট প্রয়োজনীয়তার নিরিখে যথাযথ কার্যক্রম গ্রহণের নিমিত্ত উর্ধ্বতন কর্তৃপক্ষকে অবহিত করতে হবে।

৭. তথ্য ব্যবস্থাপনা নিরীক্ষা:

প্রতিষ্ঠানের তথ্য ব্যবস্থাপনা উন্নয়নসহ যে কোনো বিপর্যয় রোধ করার ক্ষেত্রে এর নিরীক্ষা অত্যন্ত গুরুত্বপূর্ণ। গুরুত্বপূর্ণ তথ্য ব্যবস্থাপনা অবকাঠামো পরিচালনার সাথে সংশ্লিষ্ট প্রতিষ্ঠানসমূহকে অবশ্যই সময়ে সময়ে তথ্য ব্যবস্থাপনা নিরীক্ষা করতে হবে। তথ্য ব্যবস্থাপনায় বিশেষায়িত নিরীক্ষা সংস্থার মাধ্যমে নিরীক্ষা পরিচালনা করার পাশাপাশি প্রতিষ্ঠানের অভ্যন্তরীণ বিশেষজ্ঞ জনবলের মাধ্যমেও নিয়মিত নিরীক্ষা কার্যক্রম পরিচালনা করা প্রয়োজন।

৮. পরিদর্শন:

ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য-উপাত্ত সংরক্ষণসহ এগুলোর রক্ষণাবেক্ষণ করার বিষয়টি নিয়মিত তদারকি করা অত্যন্ত জরুরি। উর্ধ্বতন কর্তৃপক্ষ কর্তৃক প্রতিষ্ঠানের ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য-উপাত্ত সংরক্ষণসহ এ সকল সম্পদের ব্যবস্থাপনার বিষয়টি নিয়মিত পরিদর্শন করা প্রয়োজন।

৯. তথ্য নিরাপত্তা প্রশিক্ষণ:

প্রতিষ্ঠানের জন্য দক্ষ মানব সম্পদের গুরুত্ব অপরিসীম। দক্ষ মানব সম্পদ গড়ে তোলার জন্য যথাযথ প্রশিক্ষণ প্রয়োজন। তথ্য ও যোগাযোগ প্রযুক্তির ক্ষেত্রে সারা বিশ্বে প্রতিনিয়ত নতুন নতুন প্রযুক্তির আবির্ভাব ঘটছে। এ সকল প্রযুক্তিকে যথাযথভাবে কাজে লাগানোর জন্য সকল প্রতিষ্ঠানেই প্রশিক্ষণ কার্যক্রম চলমান রাখা প্রয়োজন। বর্তমানে সারা বিশ্বে তথ্য নিরাপত্তা একটি বড় চ্যালেঞ্জ । প্রাতিষ্ঠানিক ক্ষেত্রে তথ্য নিরাপত্তার এ চ্যালেঞ্জ মোকাবিলায় নিবিড় প্রশিক্ষণ কর্মসুচী গ্রহণ করতে হবে।

১০. 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. দি পেটেন্ট অ্যান্ড ডিজাইন অ্যাক্ট, ১৯১১;

২. রেকর্ড ম্যানুয়াল,১৯৪৩;

৩. জাতীয় আরকাইভ আইন, ১৯৮৩;

৪. কপিরাইট অ্যাক্ট, ২০০০ (২০০৫-এ সংশোধিত);

৫. তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬;

৬. তথ্য অধিকার আইন, ২০০৯;

৭. ক্রিপটোগ্রাফিক নিয়ন্ত্রণের জন্য PKI সম্পর্কিত বিধি, ২০১০;

৮. সচিবালয় নির্দেশমালা, ২০১৪;

৯. বাংলাদেশ কম্পিউটার কাউন্সির কর্তৃক প্রণিত Government of Bangladesh Information Security Manual, 2016;

১০. তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা, ২০১৮;

১১. ডিজিটাল নিরাপত্তা আইন, ২০১৮;

১২. সরকারি চাকরি আইন-২০১৮;

১৩. সরকারি ই-মেইল নীতিমালা ২০১৮;

১৪. সরকারি প্রতিষ্ঠানে সামাজিক যোগাযোগ মাধ্যম ব্যবহার সংক্রান্ত নির্দেশিকা, ২০১৯ (পরিমার্জিত সংস্করণ);