

উপ-মহাব্যবস্থাপক/
সহকারী মহাব্যবস্থাপক/
ব্যবস্থাপক
অগ্রণী ব্যাংক লিমিটেডের সকল শাখা
বাংলাদেশ।

বিষয় :- তথ্য প্রযুক্তি নীতিমালা পরিপালন প্রসঙ্গে।

তথ্য প্রযুক্তির সৃষ্টি ও নিরাপদ ব্যবহার নিশ্চিত করতে বাংলাদেশ ব্যাংক দেশের সকল ব্যাংক ও আর্থিক প্রতিষ্ঠানকে বাংলাদেশ ব্যাংকের জারীকৃত **Guideline on Information & Communication Technology for Scheduled Banks and Financial Institutions** মোতাবেক কম্পিউটার ব্যবহারে Minimum Security Standard নিশ্চিত করার লক্ষ্যে নীতিমালা প্রস্তুত পূর্বক বাস্তবায়নের নির্দেশনা প্রদান করেছে। সে মোতাবেক অত্র ব্যাংকের পরিচালনা পর্ষদ কর্তৃক ICT Policy ইতোমধ্যে অনুমোদিত হয়েছে। অগ্রণী ব্যাংক লিমিটেডের সকল শাখা ও কার্যালয়ে তথ্য ও যোগাযোগ প্রযুক্তি ব্যবহারে ব্যাংক কর্তৃপক্ষ কর্তৃক অনুমোদিত নীতিমালা অনুসরণ করার নিমিত্তে ICT Policy এর কপি প্রেরণ করা হলো। এ সম্পর্কিত Guidelines প্রস্তুত বর্তমানে চূড়ান্ত পর্যায়ে রয়েছে যা অচিরেই সংশ্লিষ্ট সকলের নিকট প্রেরণ করা হবে। এমতাবস্থায়, ICT Policy বাস্তবায়ন সংশ্লিষ্ট অতি প্রয়োজনীয় বিবেচিত বিষয়াদি সংশ্লিষ্ট সকলের অনুসরণের নিমিত্তে নিম্নে প্রদত্ত হলো:-

Documentation (নির্দেশনা লিপিবদ্ধ করন)

শাখায়/অফিসে কম্পিউটার ব্যবহারকারী সকল কর্মকর্তা/কর্মচারীর নামে কর্তব্য ও দায়-দায়িত্ব উল্লেখ করে অফিস আদেশ জারী ও সংরক্ষণ করতে হবে। অফিস আদেশে সংশ্লিষ্ট কর্মকর্তা/কর্মচারীর ছুটি/ অনুপস্থিতিতে দায়িত্ব পালনের বিষয় সুস্পষ্ট উল্লেখ থাকতে হবে। অফিস আদেশে সংশ্লিষ্ট কর্মকর্তা/কর্মচারী কোন স্তরে (User/Supervisor/Super User) কাজ করবে তা সুস্পষ্ট উল্লেখ থাকতে হবে।

শাখা সমূহের ক্ষেত্রে সংশ্লিষ্ট অফিস আদেশের একটি কপি আঞ্চলিক কার্যালয়ে এবং প্রধান কার্যালয়ের বিভিন্ন বিভাগ, সার্কেল সচিবালয়, আঞ্চলিক কার্যালয়, এডি শাখা ও কর্পোরেট শাখার ক্ষেত্রে একটি কপি সরাসরি তথ্য প্রযুক্তি বিভাগে প্রেরণ করতে হবে।

ICT Audit (আইসিটি অডিট)

বিভিন্ন শাখা/অফিসে তথ্য প্রযুক্তি বিষয়ক কার্যাবলীর নিরীক্ষা (ICT Audit) সম্পাদন করার জন্য তথ্য প্রযুক্তি বিভাগ ICT Audit Guideline তৈরী ও জারী করবে। ব্যাংকের ICT ব্যবহারকারী শাখা/অফিস Audit করণে সংশ্লিষ্ট Audit Team এ তথ্য প্রযুক্তি বিষয়ক জ্ঞান ও দক্ষতা সম্পন্ন একজন কর্মকর্তা অন্তর্ভুক্ত থাকবেন যিনি শাখা/অফিসে তথ্য ও যোগাযোগ প্রযুক্তি বিষয়ক কার্যাবলীর নিরীক্ষা (ICT Audit) সম্পাদন করবেন। শাখা/অফিস সমূহ এই সমস্ত নিরীক্ষা বিবরণীর কপি ভবিষ্যতে বাংলাদেশ ব্যাংক/প্রধান কার্যালয়/আঞ্চলিক কার্যালয়ের পর্যবেক্ষনের জন্য সংরক্ষণ করবে।

Training Procedure (প্রশিক্ষণ প্রক্রিয়া)

শাখা/অফিসে কম্পিউটার ব্যবহারকারী সকল কর্মকর্তা/কর্মচারীকে পর্যায়ক্রমে প্রয়োজনীয় প্রশিক্ষণের ব্যবস্থা গ্রহণ করতে হবে। সংশ্লিষ্ট বিভাগীয় প্রধান/আঞ্চলিক প্রধান/শাখা ব্যবস্থাপকগণ স্ব স্ব কর্মকর্তা/কর্মচারীদের প্রয়োজনীয় প্রশিক্ষণের কার্যকর ব্যবস্থা গ্রহণ করবেন।

Problem Management (সমস্যা ব্যবস্থাপনা)

কম্পিউটার হার্ডওয়ার, সফটওয়ার অথবা অন্য যে কোন কম্পিউটার সংক্রান্ত সমস্যা একটি রেজিস্টারে লিপিবদ্ধ করতে হবে। প্রথমেই সমস্যার ব্যাপারে সংশ্লিষ্ট আঞ্চলিক কার্যালয়কে অবগত করতে হবে। আঞ্চলিক কার্যালয় কর্তৃক নির্দিষ্ট সময়ের মধ্যে সমস্যা সমাধান সম্ভব না হলে এবং সমস্যাটি সফটওয়ার জনিত হলে সফটওয়ার সরবরাহকারী প্রতিষ্ঠানের সাথে রক্ষনাবেক্ষন চুক্তি থাকা সাপেক্ষে উক্ত প্রতিষ্ঠানের সাথে এবং তথ্য প্রযুক্তি বিভাগের সংশ্লিষ্ট সফটওয়ারের Help Desk এর সংশ্লিষ্ট কর্মকর্তার সাথে যোগাযোগ করতে হবে। সমস্যা হার্ডওয়ার জনিত হলে ভেভরের সাথে রক্ষনাবেক্ষন চুক্তি কিংবা যন্ত্রপাতি সমূহের ওয়ারেন্টি রয়েছে কিনা দেখতে হবে, ওয়ারেন্টি কিংবা রক্ষনাবেক্ষন চুক্তি বিদ্যমান থাকলে ভেভরের মাধ্যমে সমস্যা সমাধান করতে হবে। অন্যথায়, আঞ্চলিক কার্যালয় এর মাধ্যমে সমস্যা সমাধানের ব্যবস্থা গ্রহণ করতে হবে। অপারগতায়, প্রধান কার্যালয়ের তথ্য প্রযুক্তি বিভাগকে অবহিত করতে হবে। শাখা/আঞ্চলিক কার্যালয় ভেভর অথবা তথ্য প্রযুক্তি বিভাগকে যেকোন সমস্যা অবহিত করার জন্য Request Form (Annexure-C) ব্যবহার করতে হবে। আঞ্চলিক কার্যালয় সমূহ এ সংক্রান্ত দায়িত্ব পালনের জন্য একটি সেল গঠন করবে এবং সেখান থেকে অঞ্চলের আওতাধীন সকল শাখাকে প্রয়োজনীয় সেবা প্রদান নিশ্চিত করবে। এ সেলের দায়িত্ব পালনের জন্য একজনকে লিখিতভাবে সুনির্দিষ্ট দায়িত্ব প্রদান করতে হবে। দায়িত্বপ্রাপ্ত কর্মকর্তা/কর্মচারীর ছুটি/অনুপস্থিতিতে বিকল্প দায়িত্ব পালনের বিষয় সুস্পষ্ট উল্লেখ থাকতে হবে। ঢাকা সার্কেল

সচিবালয়, কর্পোরেট শাখা, প্রধান কার্যালয়ের বিভিন্ন বিভাগ সরাসরি তথ্য প্রযুক্তি বিভাগের সাথে যোগাযোগ করবে। ঢাকার বাইরের সার্কেল সচিবালয়, কর্পোরেট শাখা সমূহ নিকটবর্তী আঞ্চলিক কার্যালয়ের সেলের মাধ্যমে সমস্যা সমাধান করবে। হার্ডওয়ার জনিত সমস্যা তাৎক্ষণিক সমাধানের নিমিত্তে প্রতিটি আঞ্চলিক কার্যালয় ১ সেট (সিপিইউ, মনিটর, কী-বোর্ড, ইউপিএস, প্রিন্টার, পাওয়ার স্ট্রিপার) অতিরিক্ত কম্পিউটার সামগ্রী সংরক্ষণ করবে।

Change Management (পরিবর্তন ব্যবস্থাপনা)

- (ক) শাখা/ অফিসে ব্যবহৃত সফটওয়্যারের কোন পরিবর্তনের প্রয়োজন হলে নির্দিষ্ট ফরমে (Change Request Form) পরিবর্তনের জন্য আবেদন করতে হবে। ফরমের (Annexure-A) একটি নমুনা এই সঙ্গে সংযুক্ত হলো।
- (খ) কোন পরিবর্তন কার্যকর (Effective) করার আগে ব্যবহারকারীর স্বীকৃতিপত্র (User Acceptance Test-UAT) গ্রহণ করতে হবে। ব্যবহারকারীর স্বীকৃতিপত্রের নমুনা (Annexure-B) এই সঙ্গে সংযুক্ত হলো।

Asset Management (সম্পদ ব্যবস্থাপনা)

শাখার/অফিসের কম্পিউটার ও আনুসঙ্গিক যন্ত্রপাতি ও সফটওয়্যারের (কম্পিউটার এ্যাসেট) সুষ্ঠু ব্যবহার নিশ্চিত করার জন্য শাখায় একটি কম্পিউটার ইনভেন্টরী রেজিস্টার ব্যবহার করতে হবে। এ্যাসেট/ইনভেন্টরী আইটেমটি Fixed Asset (Computer) রেজিস্টারে এন্ট্রি থাক বা না থাক শাখার প্রতিটি কম্পিউটার এ্যাসেট এই রেজিস্টারে অন্তর্ভুক্ত করতে হবে। প্রতিটি এ্যাসেটের জন্য রেজিস্টারে ভিন্ন ভিন্ন পাতা ব্যবহার করতে হবে। ইনভেন্টরী রেজিস্টারে নিম্নের ছক অনুযায়ী এ্যাসেট সমূহ লিপিবদ্ধ করতে হবেঃ

এ্যাসেট কোড			কম্পিউটার সামগ্রীর বিবরণ	সরবরাহকারী প্রতিষ্ঠানের নাম	ক্রয়ের তারিখ
বিভাগ/অফিস/শাখা কোড	আইটেম কোড	ক্রমিক নং			
১	২	৩	৪	৫	৬

ওয়ারেন্টের শেষ তারিখ	ক্রয়মূল্য	বার্ষিক সমাপনীতে (৩১ ডিসেম্বর) ধার্যকৃত অবচয়	বার্ষিক সমাপনীতে (৩১ ডিসেম্বর পর্যন্ত) পুঞ্জীভূত অবচয়	বর্তমান মূল্য	মন্তব্য
৭	৮	৯	১০	১১	১২

ব্যাখ্যা :-

- ১) এ্যাসেট কোডঃ কম্পিউটার সংক্রান্ত প্রতিটি এ্যাসেটের (Asset) জন্য একটি এ্যাসেট কোড ব্যবহার করতে হবে। এ্যাসেট কোড নিম্নের তিনটি কোডের সমন্বয়ে গঠিত হবে:
- (ক) **শাখা/অঞ্চল/ সার্কেল অফিস কোড**- শাখা, আঞ্চলিক কার্যালয় এবং সার্কেল সচিবালয়ের জন্য অগ্রণী ব্যাংক লিমিটেডের প্রচলিত শাখা কোডই এখানে কোড হিসাবে ব্যবহৃত হবে। প্রধান কার্যালয়ের বিভাগ সমূহের কোড Annexure-E তে দেওয়া হলো।
- (খ) **আইটেম কোড**- নিম্নের আইটেম কোড ছকটি অনুসরণ করে আইটেম কোড বসাতে হবে।

এ্যাসেট	আইটেম কোড	এ্যাসেট	আইটেম কোড
সার্ভার	১০০১	প্যাচ পেনেল	১০১৩
সিপিইউ	১০০২	প্যাচ র‍্যাক	১০১৪
মনিটর	১০০৩	ফায়ার ওয়াল	১০১৫
ল্যাপটপ কম্পিউটার	১০০৪	রাউটার	১০১৬
ডাম্প টার্মিনাল	১০০৫	সফটওয়্যার	১০১৭
স্ক্যানার	১০০৬	মডেম	১০১৮
প্রিন্টার (ডট মেট্রিক্স)	১০০৭		-
প্রিন্টার (লেজার)	১০০৮		-
প্রিন্টার (লাইন)	১০০৯		-
ইউপিএস (অন-লাইন)	১০১০		-
ইউপিএস (অফ-লাইন)	১০১১		-
ভোল্টেজ স্ট্যাবিলাইজার	১০১২	অন্যান্য (Specify)	১০২৪

- গ) ক্রমিক নম্বর-রেজিস্টারে এন্ট্রির ক্রম অনুসারে ক্রমিক নম্বর বসাতে হবে। প্রথম আইটেমটির ক্রমিক নং ০০১ দ্বিতীয়টি ০০২ এর তৃতীয়টি ০০৩ এই ভাবে ক্রমিক নম্বর বসবে। অর্থাৎ শাখায় দুটি মনিটর থাকলে প্রথমটির ক্রমিক নং হবে- ০০১ এবং দ্বিতীয়টির ক্রমিক নং হবে-০০২।

- ২) বিবরণ- এ্যাসেটটির সংক্ষিপ্ত বিবরণ যেমনঃ- মডেল নং, ব্র্যান্ড (IBM 300 GL কম্পিউটার, EPSON LQ-2180 প্রিন্টার) ইত্যাদি।
- ৩) সরবরাহকারী- এ্যাসেটটির সরবরাহকারী প্রতিষ্ঠানের সংক্ষিপ্ত নাম।
- ৪) ক্রয়ের তারিখ - এ্যাসেটটির বিল পরিশোধের তারিখ।
- ৫) ওয়্যারেন্টি - এ্যাসেটটির ওয়্যারেন্টি শেষ হবার তারিখ।
- ৬) ক্রয়মূল্য - এ্যাসেটটির ক্রয় সংশ্লিষ্ট পরিশোধিত মূল্য।
- ৭) অবচয়- বার্ষিক সমাপনীতে (৩১ ডিসেম্বর তারিখ) ধার্যকৃত অবচয়।
- ৮) পুঞ্জীভূত অবচয়- বার্ষিক সমাপনীতে (৩১ ডিসেম্বর তারিখ পর্যন্ত) ধার্যকৃত পুঞ্জীভূত অবচয়।
- ৯) বর্তমান মূল্য - ক্রয় মূল্য থেকে পুঞ্জীভূত অবচয় বাদ দেয়ার পর অবশিষ্ট মূল্য (Book Value)।
- ১০) মন্তব্য- এ্যাসেটটির বাহ্যিক অবস্থা (ভাল/ব্যবহারযোগ্য/ব্যবহার অযোগ্য ইত্যাদি), অন্য কোথাও থেকে প্রাপ্ত কিনা ইত্যাদি লিখতে হবে।

উদাহরণ হিসাবে মনে করা যাক, লালদীঘি পূর্ব শাখা, চট্টগ্রামে ১টি IBM 300 GL সার্ভার আছে যা M/S Beximco Computers Ltd গত ০১/০১/২০০৬ তারিখে ৬০০০০.০০ টাকা মূল্যে সরবরাহ করেছে, ৩১/১২/২০০৭ তারিখে ধার্যকৃত অবচয় ১২,০০০.০০ টাকা, ৩১/১২/২০০৭ তারিখ পর্যন্ত পুঞ্জীভূত অবচয় ২৪,০০০.০০ টাকা এবং তিন বছর ওয়্যারেন্টি থাকবে। শাখার কম্পিউটার ইনভেন্টরী রেজিস্টারে নিম্নভাবে এ্যাসেটটির এন্ট্রি দিতে হবেঃ

এ্যাসেট কোড			কম্পিউটার সামগ্রীর বিবরণ(নাম ও মডেল)	সরবরাহকারী প্রতিষ্ঠানের নাম	ক্রয়ের তারিখ
বিভাগ/অফিস/শাখা কোড	আইটেম কোড	ক্রমিক নং			
১	২	৩	৪	৫	৬
২৪৫৪	১০০১	০০১	IBM 300 GL	M/S Beximco Computers Ltd	০১/০১/২০০৬

ওয়্যারেন্টির শেষ তারিখ	ক্রয়মূল্য	বার্ষিক সমাপনীতে (৩১ ডিসেম্বর) ধার্যকৃত অবচয় (টাকা)	বার্ষিক সমাপনীতে (৩১ ডিসেম্বর পর্যন্ত) পুঞ্জীভূত অবচয় (টাকা)	বর্তমান মূল্য (টাকা)	মন্তব্য
৭	৮	৯	১০	১১	১২
৩১/১২/২০০৮	৬০,০০০.০০	১২,০০০.০০	২৪,০০০.০০	৩৬,০০০.০০	সার্ভারটি সচল আছে

শাখা/অফিসের প্রত্যেকটি এ্যাসেটের গায়ে এ্যাসেট কোড অমোচনীয় এবং দৃশ্যমান কালিতে লিখতে হবে। সফটওয়্যারের ক্ষেত্রে সফটওয়্যার সিডির (যদি থাকে) উপরে এ্যাসেট নম্বর লিখতে হবে। কোন ভাবেই সিডির ডাটা পার্শ্বে (সিডি এর যে অংশে কিছু লিখা থাকে না) এ্যাসেট নম্বর লেখা যাবে না। কম্পিউটার সেট হিসাবে ক্রয় বা মূল্য পরিশোধ হয়ে থাকলে এবং তা একত্রে লিপিবদ্ধ হয়ে থাকলে প্রতিটি এ্যাসেট এর জন্য আলাদা মূল্য নির্ধারণ (Notional) করত আলাদা আলাদা ভাবে রেজিস্টারে ভুক্তি করতে হবে। উদাহরণ স্বরূপ একটি সিপিইউ ও একটি মনিটর এর (কী-বোর্ড, মাউস ইত্যাদিসহ) ক্রয় মূল্য ৪০,০০০.০০ টাকা হলে এবং তখনকার বাজার মূল্য হিসাবে সিপিইউ এর মূল্য ৩০,০০০.০০ টাকা হলে মনিটরের মূল্য ১০,০০০.০০ টাকা নির্ধারণ পূর্বক যথারীতি রেজিস্টারে ভুক্তি করতে হবে। Notional মূল্য নির্ধারণ বিষয়ে আঞ্চলিক কার্যালয়ের IT Designated কর্মকর্তার সহযোগিতা গ্রহণ করা যেতে পারে। উদাহরণে উল্লেখিত লালদীঘি পূর্ব শাখা, চট্টগ্রাম এর সার্ভার এর গায়ে এ্যাসেট কোড হবে ২৪৫৪-১০০১-০০১।

প্রধান কার্যালয়ের অডিট বিভাগ তাদের অডিট পরিচালনার সময় এবং আঞ্চলিক কার্যালয় তাদের পরিদর্শনের সময় শাখার/অফিসের প্রতিটি এ্যাসেটের গায়ে এ্যাসেট কোড লেখা আছে কিনা তা রেজিস্টারে মিলিয়ে নিশ্চিত করবে।

বার্ষিক ভিত্তিতে শাখা/অফিস/বিভাগ সমূহ স্ব স্ব শাখার/অফিসের/বিভাগের একটি ইনভেন্টরী বিবরণী পরবর্তী বৎসরের জানুয়ারী মাসের ১৫ তারিখের মধ্যে সংস্থাপন বিভাগের মাধ্যমে তথ্য প্রযুক্তি বিভাগ, প্রধান কার্যালয়, ঢাকায় পাঠাবে। প্রথম বিবরণীটি ৩১-১২-২০০৮ তারিখ ভিত্তিক আগামী ১৫-০১-২০০৯ তারিখের মধ্যে আঞ্চলিক কার্যালয়ের মাধ্যমে প্রধান কার্যালয়ের সংস্থাপন বিভাগে পৌঁছাতে হবে। প্রধান কার্যালয়ের বিভাগ সমূহ মূল্য সম্পর্কিত তথ্যাদি ব্যতিরেকে অন্যান্য তথ্য সম্বলিত রেজিস্টার সংরক্ষণ করবে এবং বর্ষ শেষে পরবর্তী বৎসরের জানুয়ারী ১৫ তারিখের মধ্যে বিবরণী সংস্থাপন বিভাগে প্রেরণ করবে। সংস্থাপন বিভাগ সকল বিভাগ ও কার্যালয়ের বিবরণী তথ্য প্রযুক্তি বিভাগে প্রেরণ করবে।

Request Management (চাহিদা ব্যবস্থাপনা)

সকল শাখা/অফিস যে কোন তথ্য-প্রযুক্তি সেবা (হার্ডওয়ার ও সফটওয়ার) এর জন্য নির্দিষ্ট ফরমে (Request Form) চাহিদা জানাবে। ফরমের একটি নমুনা এতদসঙ্গে সংযুক্ত করা হলো (Annexure-C)।

Security (নিরাপত্তা)

- (ক) সার্ভার কক্ষ অবশ্যই কাঁচের বেটন সমৃদ্ধ পার্টিসন এবং তালা সংযুক্ত হতে হবে। চাবি (যথাযথ রেকর্ড সংরক্ষণ পূর্বক) একজন দায়িত্বশীল ব্যক্তির নিকট থাকবে।
- (খ) সার্ভার কক্ষে প্রবেশাধিকার নিয়ন্ত্রিত হবে এবং সার্ভার কক্ষে রক্ষিত একটি রেজিস্টারে প্রবেশকারীদের নাম ও প্রবেশের কারণ, সময় এবং বহির্গমনের সময় লিপিবদ্ধ করতে হবে। সার্ভার কক্ষে প্রবেশ অনুমোদিত ব্যক্তিদের একটি তালিকা সংরক্ষণ করতে হবে।
- (গ) সার্ভারে অবশ্যই পাসওয়ার্ড সম্বলিত স্ক্রীন সেভার থাকতে হবে, যা দশ সেকেন্ড পরে চালু হবে।
- (ঘ) ডাটাবেজ এবং অপারেটিং সিস্টেমের এ্যাডমিনিস্ট্রেটিভ পাসওয়ার্ড একটি সীল গালাকৃত খামে ভল্টের ড্রয়ারে বিশেষ সতর্কাবে রাখতে হবে।
- (ঙ) সার্ভার কক্ষ শীতাতপ নিয়ন্ত্রিত হতে হবে। জেনারেটর ও ইউ.পি.এস এর ব্যবস্থা থাকতে হবে। সুষ্ঠু বৈদ্যুতিক ওয়্যারিং থাকতে হবে। বিদ্যুৎ এবং নেটওয়ার্ক ক্যাবলিং এর জন্য আলাদা চ্যানেল ব্যবহার করতে হবে।
- (চ) সার্ভার কক্ষ ত্যাগের পূর্বে বিদ্যুতের সুইচ অবশ্যই বন্ধ করতে হবে। সার্ভার রুমের বাহিরে অগ্নি নিরোধক যন্ত্র রাখতে হবে। বিদ্যুতের জন্য প্রয়োজনীয় আর্থিং এর ব্যবস্থা রাখতে হবে।
- (ছ) যে কম্পিউটার **Branch Banking Software** এর Workstation হিসাবে ব্যবহৃত হয় সে কম্পিউটারে কেবলমাত্র ব্যবহারকারী ডেস্কটপ পাসওয়ার্ড জানবে এবং পাসওয়ার্ড একটি সীলগালাকৃত খামে ভল্টে রাখতে হবে। কম্পিউটারে পাসওয়ার্ড সম্বলিত স্ক্রীন সেভার থাকবে, যা ১ মিনিট পর সক্রিয় হবে।
- (জ) সার্কিট ব্রেকার ও বিদ্যুৎ সরবরাহ বোর্ড ১টি তালাযুক্ত বক্সে কম্পিউটার কক্ষের বাহিরে স্থাপন করতে হবে। অগ্নি নিরোধক যন্ত্র কক্ষের বাহিরে থাকবে।

Physical Security for Desktop and Laptop Computers (ডেস্কটপ ও ল্যাপটপ কম্পিউটারের বাহ্যিক নিরাপত্তা)

- (১) ডেস্কটপ ও ল্যাপটপ কম্পিউটারের সাথে সব সময় UPS ব্যবহার করতে হবে।
- (২) ওয়ার্কস্টেশন হিসাবে ব্যবহৃত ডেস্কটপ/ল্যাপটপ কম্পিউটার যখন ব্যবহৃত হবে না (Unattended) তখন "Lock Workstation" পদ্ধতি ব্যবহার করতে হবে।
- (৩) শাখা ব্যাংকিং সফটওয়ার নেই এমন কম্পিউটারে পাসওয়ার্ড যুক্ত স্ক্রীন সেভার ব্যবহার করতে হবে যা সর্বাধিক ৫ মিনিটের মধ্যে সক্রিয় হবে।
- (৪) ডেস্কটপ/ল্যাপটপ কম্পিউটার ও মনিটর প্রতিদিন কাজের শেষে বন্ধ করতে হবে।
- (৫) যে সকল ল্যাপটপ সবসময় বা বেশীরভাগ সময়ে নেটওয়ার্কে যুক্ত থাকে সে সকল ল্যাপটপ ব্যবহারকারী বিহীন অবস্থায় রাখা যাবে না।
- (৬) ল্যাপটপ কম্পিউটার বা যে কোন প্রতিস্থাপন যোগ্য ডাটা মিডিয়া (Floppy/CD/ZIP/Flash Drive, etc.) যখন অব্যবহৃত থাকবে তখন তা একটি নিরাপদ স্থানে তালাবদ্ধ করে রাখতে হবে।
- (৭) অন্যান্য তথ্য সম্বলিত সামগ্রী যেমন কাগজ, ফাইল ইত্যাদি নিরাপদ স্থানে তালাবদ্ধ অবস্থায় রাখতে হবে।
- (৮) কোন ব্যবহারকারী কর্তৃপক্ষের অনুমোদন ব্যতিরেকে কোন Exe ফাইল অথবা Application ডেস্কটপ/ল্যাপটপ কম্পিউটার এ ইনস্টল বা ডাউনলোড করতে পারবে না।
- (৯) ডেস্কটপ/ল্যাপটপ কম্পিউটার ব্যবহারকারী কোন ক্ষতিকারক প্রোগ্রাম (Virus, Worm, Trojan etc.) তৈরী, কম্পাইল, কপি, প্রচারনা, সম্পাদন ইত্যাদি করতে পারবে না।
- (১০) যে কোন ধরনের Virus এর সন্ধান পাওয়ার সাথে সাথে প্রধান কার্যালয়, তথ্য প্রযুক্তি বিভাগকে জানাতে হবে এবং তথ্য প্রযুক্তি বিভাগের পরামর্শ অনুযায়ী প্রয়োজনীয় ব্যবস্থা নিতে হবে।
- (১১) প্রত্যেক ডেস্কটপ/ল্যাপটপ কম্পিউটার এ স্টার্ট (START) ও রিস্টার্ট (RESTART) এর সময় ইউজারের নাম এবং পাসওয়ার্ড দেয়া আবশ্যিক করতে হবে।
- (১২) সকল নিরাপত্তা জনিত ঘটনা (Security Relevant Events) লিপিবদ্ধ (Log) করার জন্য সক্ষম করে ডেস্কটপ/ল্যাপটপ কম্পিউটার কনফিগার করা থাকতে হবে।
- (১৩) ছুটির দিনে কম্পিউটার সমূহ মেঝে এবং জানালা থেকে দূরে রাখতে হবে।
- (১৪) ডেস্কটপ/ল্যাপটপ কম্পিউটারে অননুমোদিত কোন প্রকার সফটওয়ার/প্রোগ্রাম (Games, Entertainments etc.) Load/ Use করা যাবে না।
- (১৫) উর্দ্ধতন কর্তৃপক্ষের বিশেষ অনুমোদন ব্যতিরেকে ডেস্কটপ/ল্যাপটপ কম্পিউটারে ডিস্ লাইনের সংযোগ প্রদান করা যাবে না।

Information Security Standard (তথ্য নিরাপত্তা মান)**পাসওয়ার্ড নিয়ন্ত্রণ (Password Control):-**

- (ক) পাসওয়ার্ড কমপক্ষে ৬ ঘর (**Alpha** এবং **Numeric**) বিশিষ্ট হতে হবে।
- (খ) প্রত্যেক আইডিধারী প্রতি ৩০ দিনে কমপক্ষে একবার নিজ নিজ পাসওয়ার্ড অবশ্যই পরিবর্তন করবেন। নিজস্ব Password অন্য কাউকে জানানো যাবেনা।
- (গ) কোন পাসওয়ার্ড একবার ব্যবহার করলে পরবর্তী ৩ (তিন) বার সেই একই পাসওয়ার্ড ব্যবহার করা যাবে না।
- (ঘ) ইউজার আইডি এবং পাসওয়ার্ড কখনও এক হতে পারবে না।
- (ঙ) পর পর তিনবার ভুল আইডি ও পাসওয়ার্ড দিলে সিস্টেম লক হয়ে যাবে। অতএব সঠিক Password মনে রাখা নিশ্চিত করতে হবে।
- (চ) সকল লেভেলের পাসওয়ার্ড ধারী তার নিজ নিজ পাসওয়ার্ড নিজেই (সুপ্রিম ইউজার এর সাহায্য ছাড়া) পরিবর্তন করতে পারবেন।
- (ছ) সকল পাসওয়ার্ড ধারী তার পাসওয়ার্ড কঠোর গোপনীয়তার সাথে সংরক্ষণ করবেন, পাসওয়ার্ড ভুলে যাওয়া বা অপব্যবহারের দরুন ব্যাংকের কোন সুনাম বা আর্থিক ক্ষতি হলে তার দায় দায়িত্ব সংশ্লিষ্ট কর্মকর্তা/কর্মচারী এর উপর বর্তাবে।

User ID Maintenance (ব্যবহারকারীর আইডি ব্যবস্থাপনা)

কম্পিউটারের অবাধিত ব্যবহার রোধকল্পে সকল শাখা ও অফিসে ব্যাংকিং, জেনারেল লেজার ও অন্যান্য সংরক্ষিত সফটওয়্যার (Access Controlled Software) ব্যবহারকারীকে ব্যবস্থাপক/কর্তৃপক্ষ দ্বারা অনুমোদন প্রাপ্ত হতে হবে। কর্তৃপক্ষের পূর্ব অনুমোদন ছাড়া কেহ এ সমস্ত সফটওয়্যার পরিচালনা/ ব্যবহার (Operation/Use) করতে পারবে না।

শাখা ব্যবস্থাপক/কর্তৃপক্ষ প্রত্যেক কম্পিউটার ব্যবহারকারীর জন্য পৃথক পৃথক অনুমোদন পত্র Computer User Approval Form-(Annexure-D) ব্যবহার করে শাখার/অফিসের কম্পিউটার ব্যবহারকারীদের কম্পিউটার ব্যবহারের অনুমোদন প্রদান করবেন। অনুমোদন পত্রটি শাখায়/ অফিসে যথাযথভাবে সংরক্ষণ করতে হবে।

অনুমোদনপত্রে ব্যবহারকারীর ব্যক্তিগত তথ্য এবং ব্যবহারকারীর সফটওয়্যার ব্যবহারের অনুমোদন সংক্রান্ত তথ্য লিপিবদ্ধ করতে হবে। অনুমোদনপত্রে কম্পিউটার ব্যবহারকারীর ব্যক্তিগত তথ্য অংশে ব্যবহারকারীর নাম, পিতার নাম, পদবী ও কর্মরত শাখা/বিভাগের নাম, ইউজার আইডি, ব্যবহারকারীর ব্যক্তিগত নম্বর (Personnel Number) এবং অনুমোদন প্রদানকারী কর্তৃক কম্পিউটার সফটওয়্যার ব্যবহারকারীর প্রথম অনুমোদনের তারিখ লিপিবদ্ধ করতে হবে।

সফটওয়্যার ব্যবহার সংক্রান্ত তথ্যে অনুমোদনপ্রাপ্ত কর্মকর্তা/কর্মচারী কর্তৃক ব্যবহৃত কম্পিউটার সফটওয়্যারের নাম, কম্পিউটার সফটওয়্যারে ব্যবহারকারীর ইউজার লেভেল, ইউজার আইডি, কম্পিউটার সফটওয়্যার ব্যবহারকারীর বর্তমান অবস্থা (অ্যাক্টিভেট/ ডিঅ্যাক্টিভেট/ রিমুভ), অনুমোদনপ্রাপ্ত কর্মকর্তা/কর্মচারীর পূর্ণ স্বাক্ষর এবং অনুমোদন প্রদানকারীর পূর্ণ স্বাক্ষর লিপিবদ্ধ করতে হবে। সফটওয়্যার ব্যবহার সংক্রান্ত তথ্যে যখনই কোন পরিবর্তন সাধিত হবে তখন পরিবর্তন সংক্রান্ত একটি নতুন এন্ট্রি দিতে হবে। অর্থাৎ যদি ইউজার লেভেল পরিবর্তন হয় তবে একটি নতুন এন্ট্রি দিতে হবে। তদ্রূপ যদি কোন ইউজারকে অ্যাক্টিভেট/ ডিঅ্যাক্টিভেট/ রিমুভ করা হয় সেজন্যও একটি পৃথক এন্ট্রি হবে এবং প্রত্যেকটি এন্ট্রি সফটওয়্যার ব্যবহারকারী ও কর্তৃপক্ষের পূর্ণ স্বাক্ষরের মাধ্যমে প্রত্যয়িত করতে হবে।

এতদ্ব্যতিরিক্তে অনুমোদন পত্রের একটি নমুনা (Annexure-D) সংযোজিত হলো। শাখা ও অফিস সমূহ ৩১-১২-২০০৮ এর মধ্যে শাখার/অফিসের প্রত্যেক ব্যবহারকারীর জন্য পৃথক পৃথক অনুমোদনপত্র প্রদান করবে এবং তা ভবিষ্যতে নিরীক্ষার প্রয়োজনে ঘটনা ক্রমানুযায়ী যথাযথভাবে সংরক্ষণ করবে।

Virus Protection (ভাইরাস নিয়ন্ত্রণ)

প্রত্যেক ডেস্কটপ/ল্যাপটপ কম্পিউটারে Updated Virus guard ইনস্টল থাকতে হবে এবং নিয়মিত Virus চেক/অটো চেক করতে হবে। প্রত্যেক সার্ভার ও কম্পিউটারে এন্টিভাইরাস সফটওয়্যার থাকতে হবে। ভাইরাস গার্ড অটোপ্রোটেক্ট মোডে থাকবে। এন্টি ভাইরাস সফটওয়্যার সব সময় আপডেটেড থাকতে হবে। প্রত্যেক ব্যবহারকারীকে ভাইরাস সম্বন্ধে জ্ঞাত ও প্রশিক্ষিত করতে হবে।

Internet and E-mail (ইন্টারনেট ও ই-মেইল)

নেটওয়ার্ক এর সাথে যুক্ত কম্পিউটারে ইন্টারনেট সংযোগ নিতে হলে অবশ্যই ফায়ারওয়ালের মাধ্যমে সংযোগ নিতে হবে। যেকোন ই-মেইল Open করার সময় Virus চেক করতে হবে।

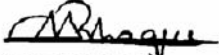
Backup/ Restore (ব্যাকআপ/রিষ্টোর)


প্রত্যেক কর্মদিবস (কম্পিউটার ভিত্তিক কাজ শেষ হওয়ার পর) শাখার/অফিসের সব ডাটার ব্যাক আপ নিতে হবে। Documentation (নির্দেশনা লিপিবদ্ধকরণ) পর্যায়ে বর্ণিত অফিস অর্ডারে ব্যাক আপের জন্য বিস্তারিত নির্দেশাবলী জারি করতে হবে। ব্যাকআপের জন্য একটি ব্যাক আপ রেজিষ্টার ব্যবহার করতে হবে যেখানে ব্যাক আপ গ্রহণকারী এবং সুপারভাইজার স্বাক্ষর করবেন। ব্যাকআপ মিডিয়াতে ব্যাকআপ ডাটা, তারিখ ইত্যাদি তথ্য স্পষ্টভাবে লিখতে হবে। ব্যাক আপ নেয়ার পর পরই ব্যাক আপের একটি কপি শাখার নিরাপদ জায়গায় রাখতে হবে। মাসিক ব্যাক আপের একটি কপি আঞ্চলিক কার্যালয়ে প্রেরণ করতে হবে এবং ষান্মাসিক ও বার্ষিক ব্যাকআপের কপি তথ্য প্রযুক্তি বিভাগে প্রেরণ করতে হবে। কমপক্ষে ত্রৈমাসিক ভিত্তিতে ব্যাক আপ রিষ্টোর করে এর কার্যকারীতা পরীক্ষা করে দেখতে হবে।

প্রত্যেক শাখা, আঞ্চলিক কার্যালয়, প্রধান কার্যালয়ের বিভাগ/অফিস সমূহকে উপরোক্ত নির্দেশনাবলী যথাযথভাবে পরিপালন করে প্রধান কার্যালয়, তথ্য প্রযুক্তি বিভাগকে নিশ্চিত করতে হবে।

উপরোক্ত বিষয়ে কোন ব্যাখ্যার প্রয়োজন হলে সরাসরি তথ্য প্রযুক্তি বিভাগের সিনিয়র সিস্টেম এনালিস্ট জনাব কাজী আলমগীর ও জনাব দেবেন্দ্র চন্দ্র দাস এবং সহকারী মহাব্যবস্থাপক জনাব মোঃ নজরুল ইসলাম এর সাথে যোগাযোগ করতে হবে।

প্রাপ্তি স্বীকার ও পরিপালন নিশ্চিত করার জন্য বলা হলো।


(মোঃ নুরুল হক)
উপ-মহাব্যবস্থাপক


(খোন্দকার মোঃ ইকবাল
মহাব্যবস্থাপক (পরিচালন)

বিতরণ :

১. ব্যবস্থাপনা পরিচালক এবং সিইও মহোদয়ের সচিবালয়, অগ্রণী ব্যাংক লিমিটেড, প্রধান কার্যালয়, ঢাকা।
২. উপ-ব্যবস্থাপনা পরিচালক -১, মহোদয়ের সচিবালয়, অগ্রণী ব্যাংক লিমিটেড, প্রধান কার্যালয়, ঢাকা।
৩. উপ-ব্যবস্থাপনা পরিচালক -২, মহোদয়ের সচিবালয়, অগ্রণী ব্যাংক লিমিটেড, প্রধান কার্যালয়, ঢাকা।
৪. সকল মহাব্যবস্থাপক, অগ্রণী ব্যাংক লিমিটেড, প্রধান কার্যালয়, ঢাকা/চট্টগ্রাম/রাজশাহী/খুলনা/বরিশাল/সিলেট।
৫. সকল বিভাগীয় প্রধান, অগ্রণী ব্যাংক লিমিটেড, প্রধান কার্যালয়, ঢাকা।
৬. পরিচালক, অগ্রণী ব্যাংক ট্রেনিং ইনস্টিটিউট, নয়াপল্টন, ঢাকা।
৭. সকল অঞ্চল প্রধান, অগ্রণী ব্যাংক লিমিটেড, আঞ্চলিক কার্যালয়, বাংলাদেশ।

সংযুক্তিঃ

১. ICT Policy (৭ পাতা),
২. Annexure A-E (৫ পাতা),
৩. Acknowledgement Receipt (১ পাতা)।

AGRANI BANK LIMITED

Information & Communication Technology (ICT) Policy



ICT POLICY 2008

1. Preamble

- 1.1 Information and Communication Technology (ICT) is a key driver for socio-economic progress and development. Promotion of ICT in various sectors of the economy is, therefore, fundamental to ensuring greater welfare of the society through efficient delivery of services. However, it is extremely important to establish transparency in the service delivery systems to make them open and visible. This is even more important in the banking sector because banks deliver services to their clients by creating products designed to suit specific needs. In addition, the significant volume of information that banking services generate requires speedier processing, storage, retrieval and dissemination for operational efficiency. To cope with these demands and to stay relevant with the pace of changes in the banking landscape, a migration to systems driven by ICT is inevitable.
- 1.2 Given the level of ICT penetration in the banking sector, it is essential that the systems developed over time are sustained, properly managed and protected from misuse and unauthorized access. This calls for a consistent policy to guide actions required to develop and upgrade ICT in banking business environment.
- 1.3 This document formulates the ICT Policy of Agrani Bank Limited (ABL) which covers all computing and communications facilities including all hardware, data, software, networks and facilities associated with information resources. The document also explains the background and constraints within which the current ICT systems were developed and presents the future built upon the experience of the past.
- 1.4 This policy is inline with the ICT guidelines issued by Bangladesh Bank for scheduled banks and financial institutions. It is supplemented by all other banks policies and by the policies of those networks to which the bank is interconnected, including applicable government laws regarding information technology.

2. Background

- 2.1 Agrani Bank Limited started using computer technology for automation of its various banking operations since pre-liberation, and many important jobs of the bank are currently automated. The Information Technology (IT) Division of the bank responsible for managing automation of banking operations is well equipped with IBM Midrange (AS400) computers and latest microcomputers and staffed with trained and experienced personnel. The bank uses its in-house software for processing most of the jobs performed in IT Division. The major jobs, handled in IT Division, includes inter-branch reconciliation, foreign bank accounts reconciliation (Nostro Accounts), consolidation of Statements of Affairs / Income & Expenditure Statements, Personnel System, Pay-roll of Head Office employees etc.
- 2.2 Agrani Bank Limited has grown significantly over the years in branch automation. Till date 241 branches out of its total 866 branches are computerized. Nine big branches of the bank are using branch banking solution in Mid-range (AS400) platform designed, developed and maintained completely by IT Division of ABL. Another 232 branches of the Bank are using LAN based Branch Banking Software supplied by 5 different vendors.
- 2.3 All 52 zonal offices of the bank have been using computers to perform day-to-day activities and are now connected with Internet. A software (Zonal Office Solution) has been developed and installed by IT Division to all the zonal offices. With this software, zonal offices compile all data related to Statement of Affairs and Profit & Loss statement from each branch under them, and send these to the Head office through internet where consolidated statements as well as various MIS reports are prepared. SWIFT Service is available in 14 AD (Authorized Dealer) branches of the bank to facilitate foreign trade operations that include quick disposal of LC's, foreign remittances etc.
- 2.4 Agrani Bank Limited has introduced ATM services for its customers since 2002. ATM card holders can withdraw cash from 19 ATM booths located at different places of Dhaka, Chittagong and Sylhet. The card holders can also make payment of utility bills such as gas, water, telephone bills using the ATM cards.
- 2.5 Agrani Bank Limited has its website (www.agranibank.org) with updated information of the Bank. Agrani Bank Limited also has its own mail server to provide e-mail facilities to concerned officials of the bank.
- 2.6 Currently, Agrani Bank is facing challenge in operating software procured from different vendors due to dissimilarity of operating procedures, and platform and consequent incompatibility. It has therefore, become necessary for the bank to take appropriate steps to migrate to its own software to be developed immediately. However, in developing or purchasing software bank should be careful about its competitiveness in the market and compatibility with the current and future business environment as well as with other banks.
- 2.7 While formulating the policies, their applicability at all tiers (Tier 1 through Tier 3) as defined in Bangladesh Bank ICT Guidelines for scheduled banks and financial institutions were taken into account.

3. ICT POLICIES

Against the backdrop as explained in the preceding section, the following policies have been formulated to realise the ICT vision of the bank.

4. Vision

To harness the potential of ICT as a key contributor to the growth and development of banking business and services of Agrani Bank Limited.

5. Scope

This ICT Policy is a subset of the Bank's corporate governance policies, providing a systematic framework around which these policies have been formulated, with particular emphasis on the security of information and information systems and also on the Communication System. This covers all aspects of information that are electronically generated, received, stored, printed, scanned, and typed.

This policy is applicable to all of the Bank's ICT systems and all activities and operations required to ensure data security including facility design, physical security, network security, disaster recovery and business continuity planning, use of hardware and software, data disposal, and protection of copyrights and other trade related aspects of intellectual property rights.

6. Objectives of the policy

- To ensure a dependable information system for efficient management and operation of the bank;
- To promote and facilitate widespread use of ICT in all banking operations;
- To use ICT to ensure enhanced efficiency in service delivery to the clients;
- To develop a large pool of trained ICT manpower to manage and sustain the systems currently in place and to be developed in future;
- To install appropriate safeguards against unauthorized access to the systems installed;
- To ensure protection of all ICT infrastructures and assets from any misuse and disaster

7. Policy Statements

The policy statements have been structured around the objectives of the policy to provide guidance for the action points required for its implementation.

7.1 Security Policy

7.1.1 Physical Security

Physical security denotes providing environmental safeguards as well as controlling physical access to equipment and data. Adequate physical securities are to be ensured for all ICT assets to prevent any loss or damage from external sources.

7.1.2 Data and Programme Security

Data and equipment should be protected from internal and external threats. Data, the most valuable asset for Bank's operations, should be protected from any level of intruder. To avoid fraud and forgery and to prevent unauthorized access, data and equipment should be maintained in a secured environment.

- Passwords should be maintained with utmost secrecy to prevent unauthorized persons from any inappropriate use of ICT resource.
- Servers which contain/store valuable computing resources of the bank should be maintained properly to prevent any kind of unauthorized intrusion or damage to it.
- Gaining access into valuable information resources from remote locations through intranet or internet is to be restricted to prevent any kind of damage to it.
- All computer users must take steps to avoid viruses and if virus is detected, immediate action is to be taken to neutralise its effect on the computer system.

7.1.3 Business Continuity and Disaster Recovery

The consequences of disaster, security failures and loss of services should be analyzed. Contingency plans should be developed and implemented to ensure that critical process could be restored within the required time scale. The plans, in turn, should be maintained and practiced as an integrated component of all other management processes. The plan should also be accepted as such by staff members, suppliers and contractors. Bank should make appropriate plans for restoration of system functions as soon as possible in case of any dislocation in the IT system. Availability of all sorts of measures like mirroring, embedded data backup system, establishment of DRS etc should be ensured.

7.2 Network Policy

The network design and its security should be implemented under documented plan and network access control as well as physical security for the network equipments should be ensured.

7.3 Internet and E-mail Policy:

All internet connections should be routed through firewall for PCs connected to network and should be separated from network dedicated to core activities of the bank to ensure integrity, reliability and confidentiality.

Email must be used carefully to avoid viruses and to avoid releasing confidential material.

7.4 Web Policy

Agrani Bank's website should be used to display only bank related information and the contents should not be modified without proper authorization.

7.5 Insurance Policy

Insurance coverage should be provided in order to minimize the costs associated with loss and/or damage to hardware/software.

7.6 Health security

Appropriate measures should be taken to keep workplaces free from radiations and other health hazards and users should be well trained about the possible health hazards of using different ICT equipment.

7.7 Procurement Policy

All procurements should be made in a transparent manner through open and competitive bidding. Where bulk procurement is possible, piecemeal procurements should be avoided. A specific outfit should be established in the headquarters to guide and manage the procurement process. Procurement should be made observing the highest standard of financial propriety to maximum economy.

7.7.1 Hardware

Hardware procurement should be made consistent with the current business requirements of the bank duly assessed by a competent committee appointed by the management.

7.7.2 Software

Bank will endeavor to purchase only the most recently upgraded versions of software and/or those in wide use in the industry and are compatible with the hardware in place.

In procuring hardware and software bank will strike a balance so that too many types are not added which may necessitate keeping too many inventories and making the system vulnerable to incompatibility.

7.8 Software Development Policy

All in-house software development activities shall be guided and monitored by the ICT Division, Agrani Bank Limited, Head Office. Security should be included at the requirement analysis stage of each development or acquisition project.

7.9 ICT Training Policy

- A detailed training needs assessment must be undertaken to identify and document training needs
- Employees should be given adequate training on the aspects of importance and awareness of ICT security before their deployment in ICT jobs.
- Training should be coordinated with the implementation of any proposed systems so that no significant delays occur between commissioning and user training

7.10 Outsourcing Policy : Certain areas of business related to ICT to bring in enhanced efficiency may be outsourced.

7.11 Business Process Re-engineering Policy

The management should commission appropriate study to redesign the business processes to achieve improvements in performance, such as cost, quality, service, and speed.

7.12 Documentation Policy

The systems already in place and to be developed further to meet future requirements should be documented according to standards set by the management. Any changes in the systems should also be appropriately reflected in the documents to facilitate further improvements in the systems design. Complete technical and user documentation must be provided for the systems together with regular updates in hard and soft copy form.

7.13 Internal ICT Audit Policy

Internal ICT Audit should be carried out periodically (at least once a year) and the report should be preserved for inspection by Bangladesh Bank officials or Bank management or persons selected from the ICT Division as and when required.

7.14 Inventory Management Policy

Inventory of all kinds of assets, such as information assets, hardware, software, licenses etc must be maintained for keeping track of all these assets. All data, equipment and associated storage media must be destroyed or overwritten before sale, disposal or reissue.

7.15 Systems Maintenance Policy

The bank should establish a support unit responsible for trouble shooting using a mechanism appropriate to ensure efficient handling of the trouble and having facility to keep records of events relating to trouble shooting.

8. Enforcement and Implementation of the Policy

Failure to adhere to the ICT Policy could result in suspension of usage privileges. Users who violate this policy will be subjected to bank's disciplinary processes and procedures including, but not limited to, those laid down in the existing Service Rules of the bank.

This policy document along with standard operating procedures should be published and made available and accessible to all concerned persons, authorities and organizations related to ICT operations in AGRANI BANK LIMITED. This policy is to be implemented phase-wise starting from the areas of priority to be decided by the management. There should be strict monitoring by the IT Division or concerned authority that the policy is being followed by the concerned persons.

9. Conclusion

This document sets out the policies taking into account the current and future business environment as well as weighing the technical issues and the alternatives available. It also focuses on the future course of information systems that is implementable and sustainable. The policy will be supplemented by a time bound action plan to take the ICT agenda forward. To respond to the emerging changes in ICT and also to ensure its continued relevance, the Policy may be amended / modified from time to time.

AGRANI BANK LIMITED
.....Branch/Division

Change Request Form

Reference :

Date :

Section I : Requester Information :

Branch/ Division Name :

Submitted by :

Change Description :

Change Purpose :

Request Date :

Section II : Approvals :

The undersigned agree and accept the change documented on this form.:

Name :

Designation :

Comments :

Date :

Signature & Seal :

Section III : Implementer Details :

The undersigned has implemented the requested change on this form:

Change reference No. :

Date of Change Implementation :

Change Implementation Details :

Was Change done successfully? Yes No.

Name :

Designation :

Signature & Seal :

(Requester)
Signature & Seal

(Head of Branch/ Division)

AGRANI BANK LIMITED
..... Branch/Division

User Acceptance Test (UAT)

Reference :

Date :

Application/ System Name :

Change Request Reference :

Date:

Test Scope (Detail plan of test):

.....
.....
.....
.....
.....
.....

Expected Result :

Actual Result :

User Acceptance Test	Fail <input type="checkbox"/>	Success <input type="checkbox"/>

Comments :

Signature & Seal :

AGRANI BANK LIMITED
.....Branch/Division

Request Form
(To be used for Problem/Request Management)

Reference :

Date :

Section I : Requester Information :

Branch/ Division Name :

Submitted by :

Contact No. :

Problem/Request
Details :

Justification :

Request Date :

Signature & Seal :
(Requester)

Signature & Seal
(Head of Branch/ Division)

Section II : Approvals :

The undersigned agree and accept the documented on this form.

Name :

Designation :

Comments :

Date :

Signature & Seal :

Section III : Implementer Details :

The undersigned has implemented the requested on this form.

Request reference No. :

Date of Request Implementation :

Request Implementation Details :

Was Request done successfully? Yes No.

Name :

Designation :

Signature & Seal :

AGRANI BANK LIMITED

Annexure-E

Division Code

Name of Division/Office	Code	Name of Division/Office	Code
Agrani Bank Training Institute	20001	Real estate & Engg. Division	20026
Audit & Inspection Division	20002	Reconciliation Division	20027
Audit Implementation Division	20003	Remittance management Division	20028
Board Division	20004	Rural Credit Division	20029
Branch Control Division	20005	SME & Micro-credit Division	20030
Central Accounts Division	20006	Chairman's Secretariat	20031
Common Services Division	20007	MD's Secretariat	20032
Currency Management Division	20008	DMD-1 Secretariat	20033
Devt. Coordination Division	20009	DMD-2 Secretariat	20034
Disciplinary Action Division	20010	GM-ID Secretariat	20035
Fund Management Division	20011	GM-Recovery Secretariat	20036
General Credit Division	20012	GM-Credit Secretariat	20037
Human Resource & Appeal Div.	20013	GM-operation Secretariat	20038
Industrial Credit-1 Division	20014	GM-Admin Secretariat	20039
Industrial Credit-2 Division	20015	GM-ID Secretariat	20040
Information Technology Division	20016	Chittagong Circle -Liason ofiice	20041
Inter. Trade Division	20017	Khulna Circle -Liason ofiice	20042
Law Division	20018	Rajshahi Circle -Liason ofiice	20043
Loan Classification Division	20019	Barisal Circle -Liason ofiice	20044
Loan Recovery Division	20020	Sylhet Circle -Liason ofiice	20045
MDS Squad Division	20021		20046
Personnel Division	20022		20047
Planning Research & MIS Division	20023		20048
Printing & Stationary Division	20024		
Public relation Division	20025		

Agrani Bank Limited

ICT Policies

Acknowledgment of ICT Policy and Instruction Circular No. IT/81 dated 15/10/2008.

This form is used to acknowledge receipt of and compliance with the Agrani Bank Limited's ICT Policy and related Instruction Circular No. IT/81 dated 15/10/2008.

Procedure:

Complete the following steps:

1. Read the ICT Policy and Instruction Circular No. IT/81 dated 15/10/2008.
2. Sign and date this form in the spaces provided below.
3. Return this page to Information Technology Division, Head Office, Dhaka.

Signature:

By signing below, I agree to the following terms:

- (i) I have received and read a copy of the ICT Policy and related Instruction Circular and understand and agree to the same.
- (ii) I understand and agree that I am not to modify, alter, or upgrade any software programs or computer equipment provided to me without the permission of the Information Technology Division.
- (iii) I understand and agree that I shall not copy, duplicate (except for backup purposes as part of my job), or allow anyone else to copy or duplicate any information or software.
- (iv) I understand and agree I must make reasonable efforts to protect all data, software and equipment from theft and physical damage.
- (v) I agree and promise to ensure Compliance of ICT Policy and related instructions contained in the Instruction Circular No. IT/81 dated 15/10/2008.

1.	_____	_____
	Signature of the Employee	Date
	_____	_____
	Name of the Employee	
	_____	_____
	Designation of the Employee	Division/Branch/Office
2.	_____	_____
	Signature of the Employee	Date
	_____	_____
	Name of the Employee	
	_____	_____
	Designation of the Employee	Division/Branch/Office
3.	_____	_____
	Signature of the Employee	Date
	_____	_____
	Name of the Employee	
	_____	_____
	Designation of the Employee	Division/Branch/Office