ડેટા એક્સેસ કંટ્રોલ પોલિસી - પોલ મર્ચન્ટ્સ ફાઇનાન્સ

વિહંગાવલોકન

નીતિ પોલ મર્ચન્ટ્સ ફાઇનાન્સ પ્રા. Ltd. (PMFPL) દિશાનિર્દેશો સુનિશ્ચિત કરવા માટે કે યોગ્ય ઍક્સેસ નિયંત્રણો અને ડેટા ગોપનીયતા લાગુ કરવામાં આવે છે અને IT અસ્કયામતો સહિત ગ્રાહકની માહિતીને સુરક્ષિત રાખવા માટે જાળવવામાં આવે છે.

અવકાશ

આ નીતિ PMFPL ના તમામ કર્મચારીઓને લાગુ પડે છે જેમાં નોન-એક્ઝિક્યુટિવ ડિરેક્ટર્સ, કામચલાઉ કર્મચારીઓ, સલાહકારો અને કરારબદ્ધ સ્ટાફનો સમાવેશ થાય છે. તમામ ઓપરેટિંગ એકમોની જવાબદારી છે કે તે સુનિશ્ચિત કરે કે આ નીતિઓ સ્પષ્ટ રીતે સંચાર કરવામાં આવે, સમજાય અને તેનું કડકપણે પાલન કરવામાં આવે. IT અસ્કયામતોની ઍક્સેસ "જાણવાની જરૂર છે" અને "એક્સેસ કરવાની જરૂર છે" આધારે આપવામાં આવે છે.

નીતિ

• જે કર્મચારીઓને સિસ્ટમ્સ અને માહિતી સંસાધનોની ઍક્સેસની જરૂર હોય તેમને ઍક્સેસ આપવામાં આવે તે પહેલાં સંબંધિત વિભાગના વડા દ્વારા તેમની ઍક્સેસ મંજૂર હોવી આવશ્યક છે. જ્યાં ડેટા જાહેર જનતા માટે મુક્તપણે ઉપલબ્ધ છે, ત્યાં ઓળખ અને પ્રમાણીકરણની જરૂર નથી.

• તમામ કર્મચારીઓને તેમની નોકરીની ભૂમિકાઓ અને જવાબદારીઓના આધારે વિવિધ અરજીઓની ઍક્સેસ આપવામાં આવે છે.

• વપરાશકર્તાઓને સક્રિય નિર્દેશિકા અમલીકરણ દ્વારા સંચાલિત કરવામાં આવશે અને દરેક વપરાશકર્તા માટે અનન્ય વપરાશકર્તા ID અને પાસવર્ડ હોવા જોઈએ.

• તમામ કર્મચારીઓને યુનિક યુઝર આઈડી અને પાસવર્ડ આપવામાં આવશે અને સિસ્ટમ એડમિનિસ્ટ્રેટર સિવાય કોઈને પણ રૂટ લોગીનની મંજૂરી આપવામાં આવશે નહીં. સિસ્ટમ એડમિનિસ્ટ્રેટર દ્વારા રૂટ લોગિનનો ઉપયોગ આઇટી મેનેજર/હેડ - આઇટી દ્વારા મંજૂર કરવામાં આવશે. સિસ્ટમ એડમિનિસ્ટ્રેટરને લગતી પ્રવૃત્તિઓ પણ લૉગ કરવામાં આવશે.

• અનધિકૃત વપરાશકર્તાઓને ઍક્સેસ નકારવામાં આવશે.

• સિસ્ટમો, નેટવર્ક્સ અને માહિતી સંસાધનોને ઍક્સેસ/મેનેજ કરવા માટે અધિકૃત તમામ કર્મચારીઓની યાદી, (તેમના ઍક્સેસના સ્તર સહિત) જાળવવામાં આવશે અને તેને અદ્યતન રાખવામાં આવશે.

ID અને પાસવર્ડ બનાવવા માટેના નિયમોનું પાલન કરવામાં આવશે.

• સિસ્ટમ એડમિનિસ્ટ્રેટર એ સુનિશ્ચિત કરશે કે PMFPL ના આંતરિક અથવા બાહ્ય નેટવર્કથી/માંથી કોઈ અવ્યવસ્થિત સીધા જોડાણો (દા.ત., અનધિકૃત મોડેમ, વાયરલેસ ઉપકરણો) નથી. કોઈપણ અપવાદોની સમીક્ષા, દસ્તાવેજીકરણ કરવામાં આવશે અને તે વિભાગના વડા દ્વારા મંજૂર કરવામાં આવશે.

• જે કર્મચારીઓને PMLPL અસ્કયામતોનો ઉપયોગ કરવા માટે અધિકૃત કરવામાં આવશે, તેમણે સાધનસામગ્રી અને માહિતીની ખોટ, નુકસાન અથવા અનધિકૃત ડેટા ઍક્સેસને રોકવા માટે તમામ વાજબી સાવચેતી રાખવી જોઈએ. આમાં પાસવર્ડ્સ, ભૌતિક સુરક્ષા સાવચેતીઓ, અનધિકૃત સૉફ્ટવેર (શેરવેર અને ફ્રીવેર) અને એન્ક્રિપ્શન પગલાંનો સમાવેશ થાય છે, પરંતુ તેના સુધી મર્યાદિત નથી.

• સિસ્ટમ એડમિનિસ્ટ્રેટર માહિતીના મૂલ્ય અને સંવેદનશીલતાને આધારે બિનઉપયોગી વિશેષાધિકારોને અક્ષમ કરવા માટે સ્વીકાર્ય સમયગાળો નક્કી કરશે.

• નેટવર્ક બંદરો અને ઉપકરણોની પસંદગીયુક્ત અથવા સુરક્ષિત ઍક્સેસ પ્રદાન કરે છે. ફ્લોપી, યુએસબી, પેનડ્રાઇવ વગેરે જેવા સ્ટોરેજ/રાઈટિંગ મીડિયાના કોઈપણ ઉપયોગને HODની પૂર્વ મંજૂરી પછી જ મંજૂરી આપવામાં આવશે અને તેનું કડક નિરીક્ષણ કરવામાં આવશે.

• પ્રતિબંધિત વિસ્તાર તરીકે જાહેર કરાયેલા વિસ્તારો નીચે મુજબના હોવા જોઈએ:

1. વિસ્તારની અંદર ફક્ત અધિકૃત કર્મચારીઓને જ મંજૂરી આપવામાં આવશે.

2. વિસ્તારમાં એક્સેસ કાર્ડ એન્ટ્રી સિસ્ટમ હોવી જોઈએ.

3. જો જરૂરી હોય તો તમામ ટેલિકોમ્યુનિકેશન સાધનો પરની વાતચીત કોઈપણ વિસંગતતા માટે રેકોર્ડ કરી શકાય છે.

• ડેટા ગોપનીયતાને સુનિશ્ચિત કરવા માટે, કોઈપણ કર્મચારીની સમાપ્તિ પર HOD એ એક્સેસ કાર્ડ્સ અને તે કર્મચારીના કબજામાં રહેલા તમામ સંબંધિત અધિકારો એકત્રિત કરશે. વધુમાં, વિભાગના યોગ્ય વરિષ્ઠને આવી સમાપ્તિ અંગે જાણ કરવામાં આવશે અને સિસ્ટમમાં તેની તમામ ઍક્સેસ (જેમ કે યુનિક યુઝર આઈડી અને પાસવર્ડ) તાત્કાલિક અસરથી નિષ્ક્રિય કરવામાં આવશે.

ગ્રાહકો અને તૃતીય પક્ષ દ્વારા ઍક્સેસ

આનો ઉદ્દેશ્ય સંસ્થા દ્વારા તેના ગ્રાહકો અને તૃતીય પક્ષોની ઍક્સેસ સંબંધિત સુરક્ષા નિયંત્રણોની રૂપરેખા આપવાનો છે.

• PMFPL પેમેન્ટ સિસ્ટમની ઍક્સેસ ફક્ત અધિકૃત ગ્રાહકો અને તેમના ગ્રાહકોને જ પ્રદાન કરવામાં આવશે.

• ગોપનીય માહિતી/સંદેશા/ફાઈલો ફક્ત સુરક્ષિત ચેનલો દ્વારા ગ્રાહકોને ટ્રાન્સફર/સંચાર કરવામાં આવશે.

જ્યારે તેઓ પ્રથમ વખત ડિફોલ્ટ પાસવર્ડ સાથે લોગ ઇન કરે ત્યારે સિસ્ટમ ક્લાયન્ટને તેમના પાસવર્ડ બદલવા માટે પ્રોમ્પ્ટ કરશે.

• ગ્રાહકોને આપવામાં આવેલ FTP ઍક્સેસ, જો કોઈ હોય તો, વપરાશકર્તાનામ અને પાસવર્ડનો ઉપયોગ કરીને સુરક્ષિત રહેશે.

• બેંકો અને અન્ય તૃતીય પક્ષો સાથે કોઈપણ માહિતી ટ્રાન્સફર અથવા અન્ય કોઈપણ સંચાર સુરક્ષિત રાખવામાં આવશે.

• ગ્રાહકો સાથેના વ્યવહારોના કોઈપણ અપૂર્ણ ટ્રાન્સમિશનને સંસ્થા દ્વારા યોગ્ય રીતે વ્યવહાર કરવામાં આવે છે.

સિસ્ટમ ત્રણ અસફળ લોગીન પ્રયાસો પર યુઝર આઈડી લોક કરવાની ખાતરી કરશે.

• ઈલેક્ટ્રોનિક વાણિજ્ય સાથે સંકળાયેલી કોઈપણ માહિતી જે સાર્વજનિક નેટવર્ક દ્વારા પસાર થતી હશે તે કપટપૂર્ણ પ્રવૃત્તિ, કરાર વિવાદ અને અનધિકૃત જાહેરાત અને ફેરફારથી સુરક્ષિત રહેશે. ઈન્ટરનેટ પર PMFPL સાથે જોડાતા તમામ ગ્રાહકો સુરક્ષિત રહેશે.

• ખોટી રૂટીંગ, અનધિકૃત મેસેજમાં ફેરફાર, અનધિકૃત જાહેરાત, અનધિકૃત મેસેજ ડુપ્લિકેશન અથવા રીપ્લે અટકાવવા માટે ઓન-લાઈન વ્યવહારો સંબંધિત માહિતી સુરક્ષિત રહેશે. આ સિસ્ટમ અને તેના સપોર્ટિંગ નેટવર્ક ઈન્ફ્રાસ્ટ્રક્ચર દ્વારા સુનિશ્ચિત કરવામાં આવે છે.

• તૃતીય પક્ષ કોન્ટ્રાક્ટરોને HOD ની પૂર્વ મંજૂરી વિના PMFPL ટેક્નોલોજી નેટવર્ક સાથે જોડાવા માટે મંજૂરી આપવામાં આવશે નહીં.

• PMFPL યોગ્ય નોન-ડિસ્ક્લોઝર એગ્રીમેન્ટ વિના તૃતીય પક્ષ કોન્ટ્રાક્ટરો સાથે ઉત્પાદન ડેટા શેર ન કરવાની ખાતરી કરશે.

• PMFPL ના નેટવર્ક સાથે જોડાયેલા તમામ તૃતીય પક્ષો PMFPL ની IT નીતિનું પાલન કરશે.

ગ્રાહકોનો ગોપનીય ડેટા

ગોપનીય ડેટા એ કાયદાઓ, નિયમો, નીતિઓ અથવા કરારની ભાષા દ્વારા સુરક્ષિત માહિતી છે. મેનેજર ડેટાને ગોપનીય તરીકે પણ નિયુક્ત કરી શકે છે. ગોપનીય ડેટા ફક્ત જાણવાની જરૂરિયાતના આધારે વ્યક્તિઓને જાહેર કરી શકાય છે. એક્ઝિક્યુટિવ મેનેજમેન્ટ અને/અથવા વાઇસ પ્રેસિડેન્ટ અને જનરલ કાઉન્સેલને PMFPL બહારના પક્ષકારોને જાહેર કરવાની અધિકૃતતા આપવી જોઈએ.

માત્ર ઉદાહરણ તરીકે, ગોપનીય ડેટાના કેટલાક ઉદાહરણોમાં નીચેનાનો સમાવેશ થાય છે:

• ગ્રાહકોનો વ્યવહાર ઇતિહાસ.

• કોઈપણ અન્ય ચુકવણી સંબંધિત માહિતી.

• સરકારી નિયમન દ્વારા ઓળખાયેલ કોઈપણ ડેટાને ગોપનીય તરીકે ગણવામાં આવે છે અથવા સક્ષમ અધિકારક્ષેત્રની કોર્ટના આદેશ દ્વારા સીલ કરવામાં આવે છે.

આવા ડેટાના સંદર્ભમાં નીચેની સાવચેતીઓ લેવામાં આવશે:

• જ્યારે ઈલેક્ટ્રોનિક ફોર્મેટમાં સંગ્રહિત કરવામાં આવે છે, ત્યારે તેને મજબૂત પાસવર્ડ્સ સાથે સુરક્ષિત કરવામાં આવશે અને નુકસાન, ચોરી, અનધિકૃત એક્સેસ અને અનધિકૃત જાહેરાત સામે રક્ષણ આપવા માટે ISS દ્વારા પ્રદાન કરાયેલ સુરક્ષા અને એન્ક્રિપ્શન પગલાં હોય તેવા સર્વર્સ પર સંગ્રહિત કરવામાં આવશે.

• સ્પષ્ટ મેનેજમેન્ટ અધિકૃતતા વિના પક્ષકારોને જાહેર કરવું જોઈએ નહીં.

• ફક્ત લૉક કરેલા ડ્રોઅર અથવા રૂમમાં અથવા એવા વિસ્તારમાં સંગ્રહિત હોવું જોઈએ જ્યાં એક્સેસને ગાર્ડ, સાઇફર લૉક અને/અથવા કાર્ડ રીડર દ્વારા નિયંત્રિત કરવામાં આવે છે, અથવા અન્યથા પર્યાપ્ત સુરક્ષા અને સભ્યો દ્વારા અનધિકૃત એક્સેસને રોકવા માટે પર્યાપ્ત ભૌતિક એક્સેસ નિયંત્રણ પગલાં હોય છે. જાહેર જનતા, મુલાકાતીઓ અથવા અન્ય વ્યક્તિઓ વિશે જાણવું જરૂરી નથી.

• જ્યારે ફેક્સ દ્વારા મોકલવામાં આવે ત્યારે ફક્ત અગાઉ સ્થાપિત અને વપરાયેલ સરનામા પર અથવા સુરક્ષિત સ્થાન તરીકે ચકાસાયેલ સરનામા પર જ મોકલવું જોઈએ.

• કોઈપણ સાર્વજનિક વેબસાઈટ પર પોસ્ટ ન કરવી જોઈએ.

• આંતરિક નીતિને આધીન હવે જરૂર ન હોય ત્યારે નાશ કરવો આવશ્યક છે. વિનાશ ફક્ત IT મેનેજર દ્વારા જ પરિપૂર્ણ થઈ શકે છે.

• હાર્ડ કોપી" સામગ્રીનો કટીંગ અથવા અન્ય પ્રક્રિયા દ્વારા નાશ થવો જોઈએ જે ડેટાને માન્યતા અથવા પુનઃનિર્માણની બહાર નષ્ટ કરે છે. વિનાશ પછી, સામગ્રીનો સામાન્ય કચરા સાથે નિકાલ થઈ શકે છે.

• ઈલેક્ટ્રોનિક સ્ટોરેજ મીડિયાને નિકાલ પહેલા ઓવરરાઈટ કરીને અથવા ડિગૉસ કરીને યોગ્ય રીતે સેનિટાઈઝ કરવામાં આવશે.

જો ગોપનીય તરીકે વર્ગીકૃત કરવામાં આવેલ ડેટા ખોવાઈ જાય, અનધિકૃત પક્ષોને જાહેર કરવામાં આવે અથવા ખોવાઈ જવાની શંકા હોય અથવા અનધિકૃત પક્ષોને જાહેર કરવામાં આવે અથવા PMFPL માહિતી પ્રણાલીઓનો કોઈ અનધિકૃત ઉપયોગ થયો હોય તો વડાની કચેરી - આઈટીને સમયસર સૂચિત કરવામાં આવશે. અથવા થવાની શંકા છે.