डेटा एक्सेस कंट्रोल पॉलिसी - पॉल मर्चेंट्स फाइनेंस

अवलोकन

नीति पॉल मर्चेंट्स फाइनेंस प्राइवेट लिमिटेड (पीएमएफपीएल) के दिशा-निर्देशों का वर्णन करती है, ताकि यह सुनिश्चित किया जा सके कि उचित एक्सेस कंट्रोल और डेटा गोपनीयता को लागू किया जाए और आईटी परिसंपत्तियों सहित ग्राहक की जानकारी की सुरक्षा के लिए बनाए रखा जाए।

क्षेत्र

यह नीति गैर-कार्यकारी निदेशकों, अस्थायी कर्मचारियों, सलाहकारों और अनुबंधित कर्मचारियों सहित सभी स्थानों पर पीएमएफपीएल के सभी कर्मचारियों पर लागू होती है। यह सुनिश्चित करना सभी परिचालन इकाइयों की जिम्मेदारी है कि इन नीतियों को स्पष्ट रूप से संप्रेषित किया जाए, समझा जाए और उनका सख्ती से पालन किया जाए। आईटी परिसंपत्तियों तक पहुंच "जानने की आवश्यकता" और "पहुंचने की आवश्यकता" के आधार पर दी जानी है।

नीति

- जिन कर्मियों को सिस्टम और सूचना संसाधनों तक पहुँच की आवश्यकता है, उन्हें पहुँच प्रदान करने से पहले संबंधित विभागाध्यक्ष द्वारा अपनी पहुँच को स्वीकृत करवाना होगा। जहाँ डेटा सार्वजनिक रूप से उपलब्ध है, वहाँ पहचान और प्रमाणीकरण की आवश्यकता नहीं हो सकती है।
- सभी कर्मियों को उनकी नौकरी की भूमिकाओं और जिम्मेदारियों के आधार पर विभिन्न अनुप्रयोगों तक पहुँच दी जाती है।
- उपयोगकर्ताओं को सक्रिय निर्देशिका कार्यान्वयन के माध्यम से प्रबंधित किया जाएगा और प्रत्येक उपयोगकर्ता के लिए अद्वितीय उपयोगकर्ता आईडी और पासवर्ड होगा।
- सभी कर्मियों को अद्वितीय उपयोगकर्ता आईडी और पासवर्ड दिया जाएगा और सिस्टम प्रशासक को छोड़कर किसी को भी रूट लॉगिन की अनुमति नहीं दी जाएगी। सिस्टम प्रशासक द्वारा रूट लॉगिन के उपयोग को आईटी प्रबंधक/आईटी प्रमुख द्वारा अनुमोदित किया जाएगा। सिस्टम प्रशासक से संबंधित गतिविधियों को भी लॉग किया जाएगा।
- अनधिकृत उपयोगकर्ताओं को पहुँच से वंचित किया जाएगा।
- सिस्टम, नेटवर्क और सूचना संसाधनों तक पहुँचने/प्रबंधित करने के लिए अधिकृत सभी कर्मियों की एक सूची (उनकी पहुँच के स्तर सहित) बनाए रखी जाएगी और उसे अद्यतित रखा जाएगा।
- आईडी और पासवर्ड बनाने के नियमों का पालन किया जाएगा।
- सिस्टम प्रशासक यह सुनिश्चित करेगा कि PMFPL के आंतरिक या बाहरी नेटवर्क से/से कोई अप्रबंधित प्रत्यक्ष कनेक्शन (जैसे, अनधिकृत मोडेम, वायरलेस डिवाइस) न हों। किसी भी अपवाद की समीक्षा की जाएगी, उसका दस्तावेजीकरण किया जाएगा और उसे विभागाध्यक्ष द्वारा अनुमोदित किया जाएगा।
- PMLPL परिसंपत्तियों का उपयोग करने के लिए अधिकृत कार्मिक उपकरण और सूचना तक हानि, क्षति या अनधिकृत डेटा पहुँच को रोकने के लिए सभी उचित सावधानी बरतेंगे। इसमें पासवर्ड, भौतिक सुरक्षा सावधानियाँ, अनधिकृत सॉफ़्टवेयर (शेयरवेयर और फ़्रीवेयर) और एन्क्रिप्शन उपाय शामिल हैं, लेकिन इन्हीं तक सीमित नहीं हैं।

- सिस्टम प्रशासक सूचना के मूल्य और संवेदनशीलता के आधार पर अप्रयुक्त विशेषाधिकारों को अक्षम करने के लिए स्वीकार्य समय अवधि निर्धारित करेगा।
- नेटवर्क पोर्ट और डिवाइस तक चुनिंदा या सुरक्षित पहुँच प्रदान करता है। फ़्लॉपी, USB, पेन ड्राइव आदि जैसे स्टोरेज/राइटिंग मीडिया के किसी भी उपयोग की अनुमति HOD की पूर्व स्वीकृति के बाद ही दी जाएगी और इसकी सख्त निगरानी की जाएगी।
- प्रतिबंधित क्षेत्र घोषित किए गए क्षेत्रों में निम्नलिखित का पालन किया जाना चाहिए:

  1. केवल अधिकृत कर्मियों को ही क्षेत्र के अंदर जाने की अनुमति होगी।

  2. क्षेत्र में एक एक्सेस कार्ड एंट्री सिस्टम होना चाहिए।

  3. यदि आवश्यक हो तो सभी दूरसंचार उपकरणों पर बातचीत को किसी भी विसंगति के लिए रिकॉर्ड किया जा सकता है।

- डेटा गोपनीयता सुनिश्चित करने के लिए, किसी भी कर्मचारी की सेवा समाप्ति पर विभागाध्यक्ष उस कर्मचारी के पास मौजूद एक्सेस कार्ड और सभी संबंधित अधिकार एकत्र करेगा। इसके अलावा, विभाग में उपयुक्त वरिष्ठ को ऐसी सेवा समाप्ति के बारे में सूचित किया जाएगा और सिस्टम तक उसकी सभी पहुँच (जैसे कि विशिष्ट उपयोगकर्ता आईडी और पासवर्ड) को तत्काल प्रभाव से निष्क्रिय कर दिया जाएगा।

ग्राहकों और तीसरे पक्ष द्वारा पहुँच

इसका उद्देश्य संगठन द्वारा अपने ग्राहकों और तीसरे पक्ष तक पहुँच के संबंध में बनाए रखने वाले सुरक्षा नियंत्रणों को रेखांकित करना है।

- PMFPL भुगतान प्रणाली तक पहुँच केवल अधिकृत ग्राहकों और उनके ग्राहकों को प्रदान की जाएगी।
- गोपनीय जानकारी/संदेश/फ़ाइलें केवल सुरक्षित चैनलों के माध्यम से ग्राहकों को हस्तांतरित/संप्रेषित की जाएंगी।
- सिस्टम ग्राहकों को उनके पासवर्ड बदलने के लिए संकेत देगा जब वे पहली बार डिफ़ॉल्ट पासवर्ड से लॉग इन करेंगे।
- ग्राहकों को प्रदान की गई FTP पहुँच, यदि कोई हो, तो उपयोगकर्ता नाम और पासवर्ड का उपयोग करके सुरक्षित की जाएगी।
- बैंकों और अन्य तीसरे पक्षों के साथ कोई भी सूचना हस्तांतरण या कोई अन्य संचार सुरक्षित रखा जाएगा।
- ग्राहकों के साथ लेनदेन के किसी भी अधूरे प्रसारण को संगठन द्वारा ठीक से निपटाया जाएगा।
- सिस्टम तीन असफल लॉगिन प्रयासों पर उपयोगकर्ता आईडी को लॉक करना सुनिश्चित करेगा।
- इलेक्ट्रॉनिक कॉमर्स से जुड़ी कोई भी जानकारी जो सार्वजनिक नेटवर्क से होकर गुजरेगी, उसे धोखाधड़ी वाली गतिविधि, अनुबंध विवाद और अनधिकृत प्रकटीकरण और संशोधन से सुरक्षित रखा जाएगा। इंटरनेट पर PMFPL से जुड़ने वाले सभी क्लाइंट सुरक्षित रहेंगे।
- ऑनलाइन लेनदेन से जुड़ी जानकारी को गलत रूटिंग, अनधिकृत संदेश परिवर्तन, अनधिकृत प्रकटीकरण, अनधिकृत संदेश दोहराव या रीप्ले को रोकने के लिए सुरक्षित रखा जाएगा। यह सिस्टम और इसके सहायक नेटवर्क इंफ्रास्ट्रक्चर द्वारा सुनिश्चित किया जाता है।
- तीसरे पक्ष के ठेकेदारों को एचओडी से पूर्व अनुमोदन के बिना पीएमएफपीएल प्रौद्योगिकी नेटवर्क से जुड़ने की अनुमति नहीं दी जाएगी।
- पीएमएफपीएल उचित गैर-प्रकटीकरण समझौते के बिना तीसरे पक्ष के ठेकेदारों के साथ उत्पादन डेटा साझा नहीं करना सुनिश्चित करेगा।

- पीएमएफपीएल के नेटवर्क से जुड़े सभी तीसरे पक्ष पीएमएफपीएल की आईटी नीति का पालन करेंगे।

ग्राहकों का गोपनीय डेटा

गोपनीय डेटा वह जानकारी है जो क़ानून, विनियमन, नीतियों या अनुबंध संबंधी भाषा द्वारा सुरक्षित होती है। प्रबंधक डेटा को गोपनीय भी घोषित कर सकते हैं। गोपनीय डेटा को केवल आवश्यकता के आधार पर व्यक्तियों को प्रकट किया जा सकता है। कार्यकारी प्रबंधन और/या उपाध्यक्ष और महाधिवक्ता को PMFPL के बाहर के पक्षों को प्रकटीकरण को अधिकृत करना चाहिए।

केवल उदाहरण के तौर पर, गोपनीय डेटा के कुछ उदाहरणों में शामिल हैं:

- ग्राहकों का लेन-देन इतिहास।
- कोई अन्य भुगतान संबंधी जानकारी।
- सरकारी विनियमन द्वारा पहचाने गए किसी भी डेटा को सक्षम न्यायालय के आदेश द्वारा गोपनीय माना जाता है या सील किया जाता है।

ऐसे डेटा के संबंध में निम्नलिखित सावधानियां बरती जानी चाहिए:

- जब इलेक्ट्रॉनिक प्रारूप में संग्रहीत किया जाता है, तो इसे मजबूत पासवर्ड से सुरक्षित किया जाना चाहिए और ऐसे सर्वर पर संग्रहीत किया जाना चाहिए जिसमें नुकसान, चोरी, अनधिकृत पहुँच और अनधिकृत प्रकटीकरण से बचाने के लिए ISS द्वारा प्रदान किए गए सुरक्षा और एन्क्रिप्शन उपाय हों।
- स्पष्ट प्रबंधन प्राधिकरण के बिना पक्षों को प्रकट नहीं किया जाना चाहिए।
- केवल लॉक किए गए दराज या कमरे या ऐसे क्षेत्र में संग्रहित किया जाना चाहिए, जहाँ पहुँच को गार्ड, सिफर लॉक और/या कार्ड रीडर द्वारा नियंत्रित किया जाता हो, या जहाँ अन्यथा पर्याप्त भौतिक पहुँच नियंत्रण उपाय हों, ताकि पर्याप्त सुरक्षा प्रदान की जा सके और जनता, आगंतुकों या अन्य व्यक्तियों द्वारा अनधिकृत पहुँच को रोका जा सके, जिन्हें इसकी जानकारी नहीं है।
- जब फ़ैक्स के माध्यम से भेजा जाता है, तो इसे केवल पहले से स्थापित और उपयोग किए गए पते पर या सुरक्षित स्थान के रूप में सत्यापित किए गए पते पर ही भेजा जाना चाहिए।
- किसी भी सार्वजनिक वेबसाइट पर पोस्ट नहीं किया जाना चाहिए।
- आंतरिक नीति के अधीन जब इसकी आवश्यकता न हो, तो इसे नष्ट कर दिया जाना चाहिए। इसे केवल आईटी प्रबंधक द्वारा ही नष्ट किया जा सकता है।
- हार्ड कॉपी" सामग्री को श्रेडिंग या किसी अन्य प्रक्रिया द्वारा नष्ट किया जाना चाहिए जो पहचान या पुनर्निर्माण से परे डेटा को नष्ट कर देता है। विनाश के बाद, सामग्री को सामान्य कचरे के साथ निपटाया जा सकता है।
- इलेक्ट्रॉनिक स्टोरेज मीडिया को निपटान से पहले ओवरराइटिंग या डीगॉसिंग द्वारा उचित रूप से साफ किया जाना चाहिए।

यदि गोपनीय के रूप में वर्गीकृत डेटा खो जाता है, अनधिकृत पक्षों को प्रकट किया जाता है या खो जाने या अनधिकृत पक्षों को प्रकट किए जाने का संदेह है, या यदि पीएमएफपीएल सूचना प्रणालियों का कोई अनधिकृत उपयोग हुआ है या होने का संदेह है, तो आईटी प्रमुख के कार्यालय को समय पर सूचित किया जाएगा।