ਡੇਟਾ ਐਕਸੈਸ ਕੰਟਰੋਲ ਨੀਤੀ - ਪਾਲ ਮਰਚੈਂਟਸ ਫਾਈਨੈਂਸ

ਸੰਖੇਪ ਜਾਣਕਾਰੀ

ਇਹ ਨੀਤੀ ਪਾਲ ਮਰਚੈਂਟਸ ਫਾਈਨਾਂਸ ਪ੍ਰਾਈਵੇਟ ਲਿਮਟਿਡ (PMFPL) ਦੇ ਦਿਸ਼ਾ-ਨਿਰਦੇਸ਼ਾਂ ਦਾ ਵਰਣਨ ਕਰਦੀ ਹੈ ਤਾਂ ਜੋ ਇਹ ਯਕੀਨੀ ਬਣਾਇਆ ਜਾ ਸਕੇ ਕਿ IT ਸੰਪਤੀਆਂ ਸਮੇਤ ਗਾਹਕ ਦੀ ਜਾਣਕਾਰੀ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਢੁਕਵੇਂ ਪਹੁੰਚ ਨਿਯੰਤਰਣ ਅਤੇ ਡੇਟਾ ਗੋਪਨੀਯਤਾ ਲਾਗੂ ਅਤੇ ਬਣਾਈ ਰੱਖੀ ਗਈ ਹੈ।

ਖੇਤਰ

ਇਹ ਨੀਤੀ ਗੈਰ-ਕਾਰਜਕਾਰੀ ਨਿਰਦੇਸ਼ਕਾਂ, ਅਸਥਾਈ ਕਰਮਚਾਰੀਆਂ, ਸਲਾਹਕਾਰਾਂ ਅਤੇ ਕੰਟਰੈਕਟ ਕਰਮਚਾਰੀਆਂ ਸਮੇਤ ਸਾਰੀਆਂ ਥਾਵਾਂ 'ਤੇ PMFPL ਦੇ ਸਾਰੇ ਕਰਮਚਾਰੀਆਂ 'ਤੇ ਲਾਗੂ ਹੁੰਦੀ ਹੈ। ਇਹ ਯਕੀਨੀ ਬਣਾਉਣਾ ਸਾਰੀਆਂ ਸੰਚਾਲਨ ਇਕਾਈਆਂ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਹੈ ਕਿ ਇਹ ਨੀਤੀਆਂ ਸਪਸ਼ਟ ਤੌਰ 'ਤੇ ਸੰਚਾਰਿਤ, ਸਮਝੀਆਂ ਅਤੇ ਸਖਤੀ ਨਾਲ ਪਾਲਣਾ ਕੀਤੀਆਂ ਜਾਣ। IT ਸੰਪਤੀਆਂ ਤੱਕ ਪਹੁੰਚ "ਜਾਣਨ ਦੀ ਲੋੜ" ਅਤੇ "ਪਹੁੰਚ ਕਰਨ ਦੀ ਲੋੜ" ਦੇ ਆਧਾਰ 'ਤੇ ਦਿੱਤੀ ਜਾਣੀ ਹੈ।

ਨੀਤੀ

ਜਿਨ੍ਹਾਂ ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਸਿਸਟਮਾਂ ਅਤੇ ਸੂਚਨਾ ਸਰੋਤਾਂ ਤੱਕ ਪਹੁੰਚ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ, ਉਹਨਾਂ ਨੂੰ ਪਹੁੰਚ ਪ੍ਰਦਾਨ ਕੀਤੇ ਜਾਣ ਤੋਂ ਪਹਿਲਾਂ ਉਹਨਾਂ ਦੀ ਪਹੁੰਚ ਨੂੰ ਸਬੰਧਤ ਵਿਭਾਗ ਦੇ ਮੁਖੀ ਦੁਆਰਾ ਪ੍ਰਵਾਨਿਤ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ। ਜਿੱਥੇ ਡੇਟਾ ਜਨਤਕ ਤੌਰ 'ਤੇ ਉਪਲਬਧ ਹੈ, ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਪਛਾਣ ਅਤੇ ਪ੍ਰਮਾਣਿਕਤਾ ਦੀ ਲੋੜ ਨਾ ਪਵੇ।

- ਸਾਰੇ ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਉਹਨਾਂ ਦੀਆਂ ਨੌਕਰੀ ਦੀਆਂ ਭੂਮਿਕਾਵਾਂ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰੀਆਂ ਦੇ ਆਧਾਰ 'ਤੇ ਵੱਖ-ਵੱਖ ਅਰਜ਼ੀਆਂ ਤੱਕ ਪਹੁੰਚ ਦਿੱਤੀ ਜਾਂਦੀ ਹੈ।
- ਉਪਭੋਗਤਾਵਾਂ ਨੂੰ ਇੱਕ ਐਕਟਿਵ ਡਾਇਰੈਕਟਰੀ ਲਾਗੂ ਕਰਨ ਦੁਆਰਾ ਪ੍ਰਬੰਧਿਤ ਕੀਤਾ ਜਾਵੇਗਾ ਅਤੇ ਹਰੇਕ ਉਪਭੋਗਤਾ ਕੋਲ ਇੱਕ ਵਿਲੱਖਣ ਉਪਭੋਗਤਾ ID ਅਤੇ ਪਾਸਵਰਡ ਹੋਵੇਗਾ।
- ਸਾਰੇ ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਯੂਨੀਕ ਯੂਜ਼ਰ ਆਈਡੀ ਅਤੇ ਪਾਸਵਰਡ ਦਿੱਤਾ ਜਾਵੇਗਾ ਅਤੇ ਸਿਸਟਮ ਪ੍ਰਸ਼ਾਸਕ ਨੂੰ ਛੱਡ ਕੇ ਕਿਸੇ ਨੂੰ ਵੀ ਰੂਟ ਲੌਗਇਨ ਦੀ ਇਜਾਜ਼ਤ ਨਹੀਂ ਦਿੱਤੀ ਜਾਵੇਗੀ। ਸਿਸਟਮ ਪ੍ਰਸ਼ਾਸਕ ਦੁਆਰਾ ਰੂਟ ਲੌਗਇਨ ਦੀ ਵਰਤੋਂ ਨੂੰ IT ਮੈਨੇਜਰ/IT ਮੁਖੀ ਦੁਆਰਾ ਮਨਜ਼ੂਰੀ ਦਿੱਤੀ ਜਾਵੇਗੀ। ਸਿਸਟਮ ਪ੍ਰਸ਼ਾਸਕ ਨਾਲ ਸਬੰਧਤ ਗਤੀਵਿਧੀਆਂ ਨੂੰ ਵੀ ਲੌਗ ਕੀਤਾ ਜਾਵੇਗਾ।
- ਅਣਅਧਿਕਾਰਤ ਉਪਭੋਗਤਾਵਾਂ ਨੂੰ ਪਹੁੰਚ ਤੋਂ ਇਨਕਾਰ ਕਰ ਦਿੱਤਾ ਜਾਵੇਗਾ।
- ਸਿਸਟਮਾਂ, ਨੈੱਟਵਰਕਾਂ ਅਤੇ ਸੂਚਨਾ ਸਰੋਤਾਂ (ਉਨ੍ਹਾਂ ਦੀ ਪਹੁੰਚ ਦੇ ਪੱਧਰਾਂ ਸਮੇਤ) ਤੱਕ ਪਹੁੰਚ/ਪ੍ਰਬੰਧਨ ਕਰਨ ਲਈ ਅਧਿਕਾਰਤ ਸਾਰੇ ਕਰਮਚਾਰੀਆਂ ਦੀ ਸੂਚੀ ਬਣਾਈ ਰੱਖੀ ਜਾਵੇਗੀ ਅਤੇ ਅੱਪ ਟੂ ਡੇਟ ਰੱਖੀ ਜਾਵੇਗੀ।
- ID ਅਤੇ ਪਾਸਵਰਡ ਬਣਾਉਣ ਲਈ ਨਿਯਮਾਂ ਦੀ ਪਾਲਣਾ ਕੀਤੀ ਜਾਵੇਗੀ।
- ਸਿਸਟਮ ਪ੍ਰਸ਼ਾਸਕ ਇਹ ਯਕੀਨੀ ਬਣਾਏਗਾ ਕਿ PMFPL ਦੇ ਅੰਦਰੂਨੀ ਜਾਂ ਬਾਹਰੀ ਨੈੱਟਵਰਕਾਂ ਨਾਲ/ਤੋਂ ਕੋਈ ਅਪ੍ਰਬੰਧਿਤ ਸਿੱਧੇ ਕਨੈਕਸ਼ਨ (ਉਦਾਹਰਨ ਲਈ, ਅਣਅਧਿਕਾਰਤ ਮਾਡਮ, ਵਾਇਰਲੈੱਸ ਡਿਵਾਈਸ) ਨਹੀਂ ਹਨ। ਕਿਸੇ ਵੀ ਅਪਵਾਦ ਦੀ ਸਮੀਖਿਆ, ਦਸਤਾਵੇਜ਼ੀ, ਅਤੇ ਵਿਭਾਗ ਦੇ ਮੁਖੀ ਦੁਆਰਾ ਮਨਜ਼ੂਰੀ ਦਿੱਤੀ ਜਾਵੇਗੀ।
- PMLPL ਸੰਪਤੀਆਂ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਲਈ ਅਧਿਕਾਰਤ ਕਰਮਚਾਰੀ ਸਾਜ਼ੋ-ਸਾਮਾਨ ਅਤੇ ਜਾਣਕਾਰੀ ਤੱਕ ਨੁਕਸਾਨ, ਨੁਕਸਾਨ ਜਾਂ ਅਣਅਧਿਕਾਰਤ ਡਾਟਾ ਪਹੁੰਚ ਨੂੰ ਰੋਕਣ ਲਈ ਸਾਰੀਆਂ ਉਚਿਤ ਸਾਵਧਾਨੀ ਵਰਤੇਗਾ। ਇਸ ਵਿੱਚ ਪਾਸਵਰਡ, ਭੌਤਿਕ ਸੁਰੱਖਿਆ ਸਾਵਧਾਨੀਆਂ, ਅਣਅਧਿਕਾਰਤ ਸੌਫਟਵੇਅਰ (ਸ਼ੇਅਰਵੇਅਰ ਅਤੇ ਫ੍ਰੀਵੇਅਰ), ਅਤੇ ਏਨਕ੍ਰਿਪਸ਼ਨ ਉਪਾਅ ਸ਼ਾਮਲ ਹਨ, ਪਰ ਇਹਨਾਂ ਤੱਕ ਸੀਮਿਤ ਨਹੀਂ ਹਨ।
- ਸਿਸਟਮ ਪ੍ਰਸ਼ਾਸਕ ਜਾਣਕਾਰੀ ਦੇ ਮੁੱਲ ਅਤੇ ਸੰਵੇਦਨਸ਼ੀਲਤਾ ਦੇ ਆਧਾਰ 'ਤੇ ਨਾ ਵਰਤੇ ਗਏ ਵਿਸ਼ੇਸ਼ ਅਧਿਕਾਰਾਂ ਨੂੰ ਅਯੋਗ ਕਰਨ ਲਈ ਇੱਕ ਸਵੀਕਾਰਯੋਗ ਸਮਾਂ ਮਿਆਦ ਨਿਰਧਾਰਤ ਕਰੇਗਾ।

- ਨੈੱਟਵਰਕ ਪੋਰਟਾਂ ਅਤੇ ਡਿਵਾਈਸਾਂ ਲਈ ਚੋਣਵੀਂ ਜਾਂ ਸੁਰੱਖਿਅਤ ਪਹੁੰਚ ਪ੍ਰਦਾਨ ਕਰਦਾ ਹੈ। ਸਟੋਰੇਜ/ਰਾਈਟਿੰਗ ਮੀਡੀਆ ਜਿਵੇਂ ਕਿ ਫਲਾਪੀ, USB, ਪੈੱਨ ਡਰਾਈਵ ਆਦਿ ਦੀ ਕਿਸੇ ਵੀ ਵਰਤੋਂ ਦੀ ਇਜਾਜ਼ਤ HOD ਦੀ ਪੂਰਵ ਪ੍ਰਵਾਨਗੀ ਤੋਂ ਬਾਅਦ ਹੀ ਦਿੱਤੀ ਜਾਵੇਗੀ ਅਤੇ ਸਖਤੀ ਨਾਲ ਨਿਗਰਾਨੀ ਕੀਤੀ ਜਾਵੇਗੀ।
- ਪ੍ਰਤਿਬੰਧਿਤ ਖੇਤਰਾਂ ਵਜੋਂ ਘੋਸ਼ਿਤ ਕੀਤੇ ਖੇਤਰਾਂ ਵਿੱਚ ਨਿਮਨਲਿਖਤ ਦੀ ਪਾਲਣਾ ਕੀਤੀ ਜਾਣੀ ਚਾਹੀਦੀ ਹੈ:

  1. ਖੇਤਰ ਦੇ ਅੰਦਰ ਸਿਰਫ਼ ਅਧਿਕਾਰਤ ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਹੀ ਇਜਾਜ਼ਤ ਦਿੱਤੀ ਜਾਵੇਗੀ।

  2. ਖੇਤਰ ਵਿੱਚ ਇੱਕ ਐਕਸੈਸ ਕਾਰਡ ਐਂਟਰੀ ਸਿਸਟਮ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ।

  3. ਜੇਕਰ ਲੋੜ ਹੋਵੇ ਤਾਂ ਸਾਰੇ ਦੂਰਸੰਚਾਰ ਯੰਤਰਾਂ 'ਤੇ ਗੱਲਬਾਤ ਨੂੰ ਕਿਸੇ ਵੀ ਅੰਤਰ ਲਈ ਰਿਕਾਰਡ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ।

- ਡੇਟਾ ਦੀ ਗੁਪਤਤਾ ਨੂੰ ਯਕੀਨੀ ਬਣਾਉਣ ਲਈ, ਕਿਸੇ ਵੀ ਕਰਮਚਾਰੀ ਦੀ ਸੇਵਾ ਸਮਾਪਤੀ 'ਤੇ ਵਿਭਾਗ ਦਾ ਮੁਖੀ ਪਹੁੰਚ ਕਾਰਡ ਅਤੇ ਉਸ ਕਰਮਚਾਰੀ ਦੁਆਰਾ ਰੱਖੇ ਗਏ ਸਾਰੇ ਸਬੰਧਤ ਅਧਿਕਾਰਾਂ ਨੂੰ ਇਕੱਠਾ ਕਰੇਗਾ। ਇਸ ਤੋਂ ਇਲਾਵਾ, ਵਿਭਾਗ ਦੇ ਉਚਿਤ ਉੱਚ ਅਧਿਕਾਰੀ ਨੂੰ ਅਜਿਹੀ ਸੇਵਾ ਦੀ ਸਮਾਪਤੀ ਬਾਰੇ ਸੂਚਿਤ ਕੀਤਾ ਜਾਵੇਗਾ ਅਤੇ ਸਿਸਟਮ (ਜਿਵੇਂ ਕਿ ਯੂਨੀਕ ਯੂਜ਼ਰ ਆਈਡੀ ਅਤੇ ਪਾਸਵਰਡ) ਤੱਕ ਉਸਦੀ ਪਹੁੰਚ ਨੂੰ ਤੁਰੰਤ ਪ੍ਰਭਾਵ ਨਾਲ ਅਯੋਗ ਕਰ ਦਿੱਤਾ ਜਾਵੇਗਾ।

ਗਾਹਕਾਂ ਅਤੇ ਤੀਜੀਆਂ ਧਿਰਾਂ ਦੁਆਰਾ ਪਹੁੰਚ

ਇਸਦਾ ਉਦੇਸ਼ ਉਹਨਾਂ ਸੁਰੱਖਿਆ ਨਿਯੰਤਰਣਾਂ ਦੀ ਰੂਪਰੇਖਾ ਤਿਆਰ ਕਰਨਾ ਹੈ ਜੋ ਸੰਗਠਨ ਆਪਣੇ ਗਾਹਕਾਂ ਅਤੇ ਤੀਜੀਆਂ ਧਿਰਾਂ ਦੁਆਰਾ ਪਹੁੰਚ ਦੇ ਸਬੰਧ ਵਿੱਚ ਰੱਖਦਾ ਹੈ।

- PMFPL ਭੁਗਤਾਨ ਪ੍ਰਣਾਲੀ ਤੱਕ ਪਹੁੰਚ ਕੇਵਲ ਅਧਿਕਾਰਤ ਗਾਹਕਾਂ ਅਤੇ ਉਹਨਾਂ ਦੇ ਗਾਹਕਾਂ ਨੂੰ ਪ੍ਰਦਾਨ ਕੀਤੀ ਜਾਵੇਗੀ।
- ਗੁਪਤ ਜਾਣਕਾਰੀ/ਸੁਨੇਹੇ/ਫਾਈਲਾਂ ਸਿਰਫ਼ ਸੁਰੱਖਿਅਤ ਚੈਨਲਾਂ ਰਾਹੀਂ ਗਾਹਕਾਂ ਨੂੰ ਟ੍ਰਾਂਸਫਰ/ਸੰਚਾਰਿਤ ਕੀਤੀਆਂ ਜਾਣਗੀਆਂ।
- ਸਿਸਟਮ ਗਾਹਕਾਂ ਨੂੰ ਆਪਣਾ ਪਾਸਵਰਡ ਬਦਲਣ ਲਈ ਪੁੱਛੇਗਾ ਜਦੋਂ ਉਹ ਪਹਿਲੀ ਵਾਰ ਡਿਫੌਲਟ ਪਾਸਵਰਡ ਨਾਲ ਲੌਗਇਨ ਕਰਨਗੇ।
- ਗਾਹਕਾਂ ਨੂੰ ਪ੍ਰਦਾਨ ਕੀਤੀ FTP ਪਹੁੰਚ, ਜੇਕਰ ਕੋਈ ਹੈ, ਇੱਕ ਉਪਭੋਗਤਾ ਨਾਮ ਅਤੇ ਪਾਸਵਰਡ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਸੁਰੱਖਿਅਤ ਕੀਤੀ ਜਾਵੇਗੀ।
- ਬੈਂਕਾਂ ਅਤੇ ਹੋਰ ਤੀਜੀਆਂ ਧਿਰਾਂ ਨਾਲ ਕੋਈ ਵੀ ਜਾਣਕਾਰੀ ਟ੍ਰਾਂਸਫਰ ਜਾਂ ਕੋਈ ਹੋਰ ਸੰਚਾਰ ਸੁਰੱਖਿਅਤ ਰੱਖਿਆ ਜਾਵੇਗਾ।
- ਗਾਹਕਾਂ ਦੇ ਨਾਲ ਲੈਣ-ਦੇਣ ਦੇ ਕਿਸੇ ਵੀ ਅਧੂਰੇ ਸੰਚਾਰ ਨੂੰ ਸੰਗਠਨ ਦੁਆਰਾ ਸਹੀ ਢੰਗ ਨਾਲ ਨਜਿੱਠਿਆ ਜਾਵੇਗਾ।
- ਸਿਸਟਮ ਤਿੰਨ ਅਸਫਲ ਲੌਗਇਨ ਕੋਸ਼ਿਸ਼ਾਂ 'ਤੇ ਉਪਭੋਗਤਾ ID ਨੂੰ ਲਾਕ ਕਰਨਾ ਯਕੀਨੀ ਬਣਾਏਗਾ।
- ਇਲੈਕਟ੍ਰਾਨਿਕ ਕਾਮਰਸ ਨਾਲ ਸਬੰਧਤ ਕੋਈ ਵੀ ਜਾਣਕਾਰੀ ਜੋ ਜਨਤਕ ਨੈੱਟਵਰਕਾਂ ਵਿੱਚੋਂ ਲੰਘਦੀ ਹੈ, ਧੋਖਾਧੜੀ ਵਾਲੀ ਗਤੀਵਿਧੀ, ਇਕਰਾਰਨਾਮੇ ਦੇ ਵਿਵਾਦਾਂ, ਅਤੇ ਅਣਅਧਿਕਾਰਤ ਖੁਲਾਸੇ ਅਤੇ ਸੋਧਾਂ ਤੋਂ ਸੁਰੱਖਿਅਤ ਕੀਤੀ ਜਾਵੇਗੀ। ਇੰਟਰਨੈੱਟ 'ਤੇ PMFPL ਨਾਲ ਜੁੜਨ ਵਾਲੇ ਸਾਰੇ ਗਾਹਕ ਸੁਰੱਖਿਅਤ ਹੋਣਗੇ।
- ਗਲਤ ਰੂਟਿੰਗ, ਅਣਅਧਿਕਾਰਤ ਸੰਦੇਸ਼ ਵਿੱਚ ਤਬਦੀਲੀ, ਅਣਅਧਿਕਾਰਤ ਖੁਲਾਸਾ, ਅਣਅਧਿਕਾਰਤ ਸੰਦੇਸ਼ ਡੁਪਲੀਕੇਸ਼ਨ ਜਾਂ ਰੀਪਲੇ ਨੂੰ ਰੋਕਣ ਲਈ ਔਨਲਾਈਨ ਲੈਣ-ਦੇਣ ਨਾਲ ਸਬੰਧਤ ਜਾਣਕਾਰੀ ਸੁਰੱਖਿਅਤ ਕੀਤੀ ਜਾਵੇਗੀ। ਇਹ ਸਿਸਟਮ ਅਤੇ ਇਸਦੇ ਸਹਾਇਕ ਨੈੱਟਵਰਕ ਬੁਨਿਆਦੀ ਢਾਂਚੇ ਦੁਆਰਾ ਯਕੀਨੀ ਬਣਾਇਆ ਜਾਂਦਾ ਹੈ।
- ਤੀਜੀ ਧਿਰ ਦੇ ਠੇਕੇਦਾਰਾਂ ਨੂੰ HOD ਤੋਂ ਪੂਰਵ ਪ੍ਰਵਾਨਗੀ ਤੋਂ ਬਿਨਾਂ PMFPL ਤਕਨਾਲੋਜੀ ਨੈੱਟਵਰਕ ਨਾਲ ਜੁੜਨ ਦੀ ਇਜਾਜ਼ਤ ਨਹੀਂ ਦਿੱਤੀ ਜਾਵੇਗੀ।
- PMFPL ਉਚਿਤ ਗੈਰ-ਖੁਲਾਸਾ ਸਮਝੌਤੇ ਤੋਂ ਬਿਨਾਂ ਤੀਜੀ ਧਿਰ ਦੇ ਠੇਕੇਦਾਰਾਂ ਨਾਲ ਉਤਪਾਦਨ ਡੇਟਾ ਨੂੰ ਸਾਂਝਾ ਨਾ ਕਰਨਾ ਯਕੀਨੀ ਬਣਾਏਗਾ।
- PMFPL ਦੇ ਨੈੱਟਵਰਕ ਨਾਲ ਜੁੜੀਆਂ ਸਾਰੀਆਂ ਤੀਜੀਆਂ ਧਿਰਾਂ PMFPL ਦੀ IT ਨੀਤੀ ਦੀ ਪਾਲਣਾ ਕਰਨਗੀਆਂ।

ਗੁਪਤ ਗਾਹਕ ਡਾਟਾ

ਗੁਪਤ ਡੇਟਾ ਉਹ ਜਾਣਕਾਰੀ ਹੁੰਦੀ ਹੈ ਜੋ ਕਾਨੂੰਨ, ਨਿਯਮ, ਨੀਤੀਆਂ, ਜਾਂ ਇਕਰਾਰਨਾਮੇ ਦੀ ਭਾਸ਼ਾ ਦੁਆਰਾ ਸੁਰੱਖਿਅਤ ਹੁੰਦੀ ਹੈ। ਮੈਨੇਜਰ ਡੇਟਾ ਨੂੰ ਗੁਪਤ ਘੋਸ਼ਿਤ ਵੀ ਕਰ ਸਕਦੇ ਹਨ। ਗੁਪਤ ਡੇਟਾ ਦਾ ਖੁਲਾਸਾ ਸਿਰਫ਼ ਲੋੜ-ਤੋਂ-ਲੋੜ ਦੇ ਆਧਾਰ 'ਤੇ ਵਿਅਕਤੀਆਂ ਨੂੰ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ। ਕਾਰਜਕਾਰੀ ਪ੍ਰਬੰਧਨ ਅਤੇ/ਜਾਂ ਵਾਈਸ ਪ੍ਰੈਜ਼ੀਡੈਂਟ ਅਤੇ ਜਨਰਲ ਕਾਉਂਸਲ ਨੂੰ PMFPL ਤੋਂ ਬਾਹਰਲੀਆਂ ਪਾਰਟੀਆਂ ਨੂੰ ਖੁਲਾਸਾ ਕਰਨ ਦਾ ਅਧਿਕਾਰ ਦੇਣਾ ਚਾਹੀਦਾ ਹੈ।

ਕੇਵਲ ਉਦਾਹਰਨ ਦੇ ਰੂਪ ਵਿੱਚ, ਗੁਪਤ ਡੇਟਾ ਦੀਆਂ ਕੁਝ ਉਦਾਹਰਣਾਂ ਵਿੱਚ ਸ਼ਾਮਲ ਹਨ:

1. ਗਾਹਕ ਲੈਣ-ਦੇਣ ਦਾ ਇਤਿਹਾਸ।
2. ਭੁਗਤਾਨ ਸੰਬੰਧੀ ਕੋਈ ਹੋਰ ਜਾਣਕਾਰੀ।
3. ਸਰਕਾਰੀ ਨਿਯਮਾਂ ਦੁਆਰਾ ਪਛਾਣੇ ਗਏ ਕਿਸੇ ਵੀ ਡੇਟਾ ਨੂੰ ਗੁਪਤ ਮੰਨਿਆ ਜਾਂਦਾ ਹੈ ਜਾਂ ਸਮਰੱਥ ਅਦਾਲਤ ਦੇ ਆਦੇਸ਼ ਦੁਆਰਾ ਸੀਲ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।

ਅਜਿਹੇ ਡੇਟਾ ਦੇ ਸਬੰਧ ਵਿੱਚ ਹੇਠ ਲਿਖੀਆਂ ਸਾਵਧਾਨੀਆਂ ਵਰਤਣੀਆਂ ਚਾਹੀਦੀਆਂ ਹਨ:

- ਜਦੋਂ ਇਲੈਕਟ੍ਰਾਨਿਕ ਫਾਰਮੈਟ ਵਿੱਚ ਸਟੋਰ ਕੀਤਾ ਜਾਂਦਾ ਹੈ, ਤਾਂ ਇਸਨੂੰ ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਨਾਲ ਸੁਰੱਖਿਅਤ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ ਅਤੇ ਇੱਕ ਸਰਵਰ 'ਤੇ ਸਟੋਰ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ ਜਿਸ ਵਿੱਚ ਨੁਕਸਾਨ, ਚੋਰੀ, ਅਣਅਧਿਕਾਰਤ ਪਹੁੰਚ ਅਤੇ ਅਣਅਧਿਕਾਰਤ ਖੁਲਾਸੇ ਤੋਂ ਸੁਰੱਖਿਆ ਲਈ ISS ਦੁਆਰਾ ਪ੍ਰਦਾਨ ਕੀਤੇ ਗਏ ਸੁਰੱਖਿਆ ਅਤੇ ਐਨਕ੍ਰਿਪਸ਼ਨ ਉਪਾਅ ਹੋਣ।
- ਪਾਰਟੀਆਂ ਨੂੰ ਸਪੱਸ਼ਟ ਪ੍ਰਬੰਧਨ ਅਧਿਕਾਰ ਤੋਂ ਬਿਨਾਂ ਖੁਲਾਸਾ ਨਹੀਂ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ।
- ਕੇਵਲ ਇੱਕ ਤਾਲਾਬੰਦ ਦਰਾਜ਼ ਜਾਂ ਕਮਰੇ ਜਾਂ ਖੇਤਰ ਵਿੱਚ ਸਟੋਰ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ ਜਿੱਥੇ ਪਹੁੰਚ ਨੂੰ ਗਾਰਡ, ਸਿਫਰ ਲਾਕ ਅਤੇ/ਜਾਂ ਕਾਰਡ ਰੀਡਰ ਦੁਆਰਾ ਨਿਯੰਤਰਿਤ ਕੀਤਾ ਜਾਂਦਾ ਹੈ, ਜਾਂ ਜਿੱਥੇ ਢੁਕਵੀਂ ਸੁਰੱਖਿਆ ਪ੍ਰਦਾਨ ਕਰਨ ਅਤੇ ਅਣਅਧਿਕਾਰਤ ਪਹੁੰਚ ਨੂੰ ਰੋਕਣ ਲਈ ਢੁਕਵੇਂ ਸਰੀਰਕ ਪਹੁੰਚ ਨਿਯੰਤਰਣ ਉਪਾਅ ਮੌਜੂਦ ਹਨ ਜਨਤਕ, ਵਿਜ਼ਟਰ ਜਾਂ ਹੋਰ ਵਿਅਕਤੀ ਜੋ ਇਸ ਬਾਰੇ ਨਹੀਂ ਜਾਣਦੇ ਹਨ।
- ਫੈਕਸ ਰਾਹੀਂ ਭੇਜਣ ਵੇਲੇ, ਇਹ ਸਿਰਫ਼ ਪਹਿਲਾਂ ਹੀ ਸਥਾਪਿਤ ਅਤੇ ਵਰਤੇ ਗਏ ਪਤੇ 'ਤੇ ਜਾਂ ਕਿਸੇ ਸੁਰੱਖਿਅਤ ਟਿਕਾਣੇ ਵਜੋਂ ਪ੍ਰਮਾਣਿਤ ਪਤੇ 'ਤੇ ਭੇਜਿਆ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ।
- ਕਿਸੇ ਵੀ ਜਨਤਕ ਵੈੱਬਸਾਈਟ 'ਤੇ ਪੋਸਟ ਨਹੀਂ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ।
- ਅੰਦਰੂਨੀ ਨੀਤੀ ਦੇ ਅਧੀਨ, ਇਸਦੀ ਲੋੜ ਨਾ ਹੋਣ 'ਤੇ ਇਸਨੂੰ ਨਸ਼ਟ ਕਰ ਦੇਣਾ ਚਾਹੀਦਾ ਹੈ। ਇਸਨੂੰ ਸਿਰਫ਼ ਆਈ.ਟੀ. ਮੈਨੇਜਰ ਦੁਆਰਾ ਹੀ ਮਿਟਾਇਆ ਜਾ ਸਕਦਾ ਹੈ।
- "ਹਾਰਡ ਕਾਪੀ" ਸਮੱਗਰੀ ਨੂੰ ਕੱਟਣ ਜਾਂ ਕਿਸੇ ਹੋਰ ਪ੍ਰਕਿਰਿਆ ਦੁਆਰਾ ਨਸ਼ਟ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ ਜੋ ਪਛਾਣ ਜਾਂ ਪੁਨਰ ਨਿਰਮਾਣ ਤੋਂ ਪਰੇ ਡੇਟਾ ਨੂੰ ਨਸ਼ਟ ਕਰ ਦਿੰਦੀ ਹੈ, ਸਮੱਗਰੀ ਨੂੰ ਆਮ ਕੂੜੇ ਨਾਲ ਨਿਪਟਾਇਆ ਜਾ ਸਕਦਾ ਹੈ।
- ਨਿਪਟਾਰੇ ਤੋਂ ਪਹਿਲਾਂ ਇਲੈਕਟ੍ਰਾਨਿਕ ਸਟੋਰੇਜ ਮੀਡੀਆ ਨੂੰ ਓਵਰਰਾਈਟਿੰਗ ਜਾਂ ਡੀਗੌਸਿੰਗ ਦੁਆਰਾ ਸਹੀ ਤਰ੍ਹਾਂ ਸਾਫ਼ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ।
- ਜੇਕਰ ਗੁਪਤ ਦੇ ਤੌਰ 'ਤੇ ਵਰਗੀਕ੍ਰਿਤ ਡੇਟਾ ਗੁੰਮ ਹੋ ਜਾਂਦਾ ਹੈ, ਅਣਅਧਿਕਾਰਤ ਪਾਰਟੀਆਂ ਨੂੰ ਖੁਲਾਸਾ ਕੀਤਾ ਜਾਂਦਾ ਹੈ ਜਾਂ ਅਣਅਧਿਕਾਰਤ ਪਾਰਟੀਆਂ ਨੂੰ ਗੁੰਮ ਜਾਂ ਪ੍ਰਗਟ ਹੋਣ ਦਾ ਸ਼ੱਕ ਹੈ, ਜਾਂ ਜੇਕਰ PMFPL ਸੂਚਨਾ ਪ੍ਰਣਾਲੀਆਂ ਦੀ ਕੋਈ ਅਣਅਧਿਕਾਰਤ ਵਰਤੋਂ ਹੋਈ ਹੈ ਜਾਂ ਹੋਣ ਦਾ ਸ਼ੱਕ ਹੈ, ਤਾਂ IT ਮੁਖੀ ਦੇ ਦਫ਼ਤਰ ਨੂੰ ਸੂਚਿਤ ਕੀਤਾ ਜਾਵੇਗਾ। ਸਮੇਂ ਵਿੱਚ.