राष्ट्रीय कृषि और ग्रामीण विकास बैंक

नाबार्ड

साइबरसुरक्षा हैंडबुक 2.0

प्रभावी साइबर सुरक्षा हेतु रणनीतियाँ

विषय

वस्तु

डेटाबेस सुरक्षा

डेटाबेस सुरक्षा गोपनीयता और अखंडता सुनिश्चित करते हुए, अनधिकृत पहुँच, हमलों और हानि से डेटा की सुरक्षा के लिए नीतियों और नियंत्रणों का उपयोग करती है.

घटना प्रबंधन

घटना प्रबंधन व्यावसायिक प्रभाव को न्यूनतम करने तथा रिकवरी सुनिश्चित करने के लिए सुरक्षा खतरों का पता लगाने, उनका विश्लेषण करने तथा समाधान करने की व्यवस्थित प्रक्रिया है.

तृतीय पक्ष सुरक्षा प्रबंधन

तृतीय-पक्ष सुरक्षा प्रबंधन डेटा, प्रणाली और अनुपालन की सुरक्षा के लिए विक्रेताओं और भागीदारों से जोखिमों की पहचान करता है, उनका शमन और अनुप्रवर्तन करता है.

नेटवर्क सुरक्षा

नेटवर्क सुरक्षा, नेटवर्क की अखंडता और डेटा को अनधिकृत पहुँच, दुरुपयोग और साइबर हमलों से बचाने के लिए प्रौद्योगिकियों, नियंत्रणों और नीतियों का उपयोग करती है.

प्रशिक्षण और जागरूकता

साइबर सुरक्षा प्रशिक्षण और जागरूकता साइबर खतरों को पहचानने, रोकने और उनका जवाब देने, जोखिमों का शमन करने और संगठनात्मक सुरक्षा को बढ़ाने के लिए शिक्षित करती है.

एक्सैस कंट्रोल और पैच प्रबंधन

एक्सेस कंट्रोल अधिकृत उपयोगकर्ताओं/ डिवाइसों तक नेटवर्क पहुँच को प्रतिबंधित करता है, जबकि पैच प्रबंधन भेद्यताओं को ठीक करने और सुरक्षा बढ़ाने के लिए सिस्टम को अपडेट करता है.

आस्ति प्रबंधन

आस्ति प्रबंधन जोखिमों और कमजोरियों का शमन करने के लिए किसी संगठन की डिजिटल और भौतिक आस्तियों की पहचान, ट्रैकिंग और सुरक्षा करने की निरंतर प्रक्रिया है.

नाबार्ड

डेटाबेस सुरक्षा

क्या करें

नियमित अपडेट

जैसे ही पैच और अपग्रेड उपलब्ध हों, उनका उपयोग डेटाबेस इंजन और उसके साथ काम करने वाले किसी भी सॉफ्टवेयर में सुरक्षा संबंधी कमियों को दूर करने के लिए करें.

डेटा एंक्रिप्ट करना

निजी जानकारी को उन लोगों से सुरक्षित रखने के लिए, जिनके पास उसका एक्सैस नहीं होना चाहिए, ऐसे डेटा पर एन्क्रिप्शन का उपयोग करें जो स्थिर है और पारगमन में है.

एक्सैस कंट्रोल कार्यान्वित करना

भूमिका-आधारित एक्सैस और न्यूनतम विशेषाधिकार की धारणा का उपयोग कर यह सीमित करें कि कौन डेटा देख सकता है, बदल सकता है या हटा सकता है.

गतिविधि का अनुप्रवर्तन

लॉगिंग चालू करें और प्रायः ऑडिट ट्रेल्स की जाँच करें, ताकि यह पता चल सके कि कहीं कोई व्यक्ति संदिग्ध अनुरोध तो नहीं कर रहा है या बिना अनुमति के डेटा एक्सैस करने का प्रयास तो नहीं कर रहा है.

डेटाबेस बैकअप

अपने बैकअप की नियमित रूप से प्रतिलिपियाँ बनाएँ और उन्हें सुरक्षित रखने के लिए सुरक्षित रूप से संग्रहित करें. साथ ही, यह भी देखें कि क्या वे एन्क्रिप्टेड हैं और उन्हें पुनःस्थापित किया जा सकता है.

सुदृढ़ प्रमाणीकरण का उपयोग करें

सुनिश्चित करें कि डेटाबेस ऐडमिन और विशेष एक्सैस वाले अन्य उपयोगकर्ता बहु-कारक प्रमाणीकरण का उपयोग करें.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

डेटाबेस सुरक्षा

क्या न करें!

डिफ़ॉल्ट क्रिडेंशियल्स का उपयोग न करें

तुरंत डिफ़ॉल्ट यूज़र और पासवर्ड बदलें. सुरक्षा की दृष्टि से ऐसा न करना काफ़ी जोखिम भरा हो सकता है.

संवेदनशील डेटा को सादे टेक्स्ट में न रखें

अपने पासवर्ड, व्यक्तिगत जानकारी या वित्तीय जानकारी को सादे टेक्स्ट में न रखें. इसके बजाय उन्हें एन्क्रिप्शन से सुरक्षित रखें.

उपयोगकर्ताओं को बहुत अधिक अधिकार न दें

उपयोगकर्ताओं को केवल उतना ही एक्सैस प्रदान करें जितनी उन्हें आवश्यकता है तथा उन्हें ऐडमिन के अधिकार केवल तब ही प्रदान करें जब उन्हें वास्तव में इसकी आवश्यकता हो.

लॉग और अलर्ट को नज़रअंदाज़ न करें

अगर आप लॉग्स की जाँच नहीं करते, तो आप उल्लंघनों को नज़रअंदाज़ कर सकते हैं. आपको हमेशा उन चीज़ों पर ध्यान देना चाहिए जो संदिग्ध लगती हैं.

बैकअप सुरक्षा के बारे में न भूलें

हमलावरों को असुरक्षित बैकअप पसंद आते हैं. उन्हें ऐसी जगहों पर न रखें जो सुरक्षित न हों या जहाँ पहुँचना आसान न हो.

परीक्षण न छोड़ें

हमेशा सुनिश्चित करें कि आपका डेटाबेस सुरक्षित है और आपको बैकअप को पुनःस्थापित करने का उपाय पता है.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

घटना प्रबंधन

क्या करें

स्पष्ट प्रक्रियाएँ निर्धारित करें

सुनिश्चित करें कि समस्याओं का पता लगाने, उन्हें रिपोर्ट करने और उन्हें ठीक करने के लिए स्पष्ट और लिखित चरण मौजूद हों. सभी को पता होना चाहिए कि उन्हें क्या करना है.

प्रभाव के आधार पर प्राथमिकता तय करें

यह सुनिश्चित करने के लिए कि सबसे महत्वपूर्ण बातों का पहले ध्यान रखा जाए, उन्हें इस आधार पर वर्गीकृत करें कि वे कितनी गंभीर हैं और उनका संगठन पर क्या प्रभाव पड़ता है.

एक मजबूत प्रतिक्रिया टीम बनाएं

एक मजबूत प्रतिक्रिया टीम बनाने के लिए कुशल कर्मियों को तकनीकी प्रतिक्रियाकर्ता आदि जैसी विशिष्ट भूमिकाएँ दें.

स्वचालन और अनुप्रवर्तन उपकरणों का उपयोग करें

ऐसी प्रौद्योगिकियों का उपयोग करें जो आपको वास्तविक समय में अलर्ट प्रदान करें, लॉग की जाँच करें, तथा स्वचालित रूप से टिकट जारी करें, ताकि आपको समस्याओं का पता लगाने और उन्हें तेजी से ठीक करने में सहायता मिल सके.

अपने रिकॉर्ड को अद्यतन रखें

भविष्य में संदर्भ और अनुपालन के लिए, सुनिश्चित करें कि आपके पास स्पष्ट रिकॉर्ड हो कि क्या हुआ, आपने इसका कारण कैसे पता लगाया, तथा इसे सुधारने के लिए आपने क्या किया.

घटना के बाद समीक्षा करें

किसी घटना के बाद, यह देखने के लिए वापस जाएँ कि क्या गलत हुआ, क्या कारगर रहा, तथा भविष्य में प्रतिक्रियाओं को कैसे बेहतर बनाया जा सकता है.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

घटना प्रबंधन

क्या न करें!

जवाब देने के लिए बहुत लंबा इंतज़ार न करें

समय बहुत महत्वपूर्ण है. आप जितनी देर करेंगे, नुकसान उतना ही ज़्यादा होगा और उसे ठीक करने में भी उतना ही ज़्यादा समय लगेगा.

दस्तावेज़ीकरण न छोड़ें

यदि आप किसी घटना का विवरण नहीं लिखेंगे तो नियमों का पालन करना और बाद में यह समझना कठिन हो जाएगा कि क्या हो रहा है.

छोटे अलर्ट को नज़रअंदाज़ न करें

छोटी-छोटी समस्याओं का मतलब है कि बड़ी समस्याएँ आने वाली हैं. इससे पहले कि हालात हाथ से निकल जाएँ, उन पर गौर करें.

बात करना न भूलें

जब लोग किसी कार्यक्रम के दौरान बात नहीं करते, तो यह समझना कठिन हो जाता है कि क्या हो रहा है. लोगों को समय पर बताएँ कि क्या हो रहा है ताकि हर कोई जागरूक हो सके.

प्रशिक्षण की उपेक्षा न करें

अपनी टीमों को प्रशिक्षित करना न भूलें. अगर उन्हें प्रशिक्षित नहीं किया गया, तो वे किसी घटना के दौरान घबरा सकते हैं या ग़लतियाँ कर सकते हैं. नियमित रूप से प्रशिक्षण देना आवश्यक है.

अपनी योजना बदलना न भूलें

जैसे-जैसे व्यवस्थाएँ बदलती हैं, वैसे-वैसे कठिनाइयों से निपटने की आपकी योजना भी बदलनी चाहिए. सुनिश्चित करें कि यह अद्यतित रहे.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

तृतीय पक्ष सुरक्षा प्रबंधन

क्या करें

सम्यक तत्परता से जाँच करें

किसी विक्रेता को लाने से पहले, उनके प्रमाणपत्रों, प्रक्रियाओं और उल्लंघनों के इतिहास की जाँच कर लें कि वे कितने सुरक्षित हैं.

स्पष्ट सुरक्षा आवश्यकता निर्धारित करें

संविदाओं और एसएलए में स्पष्ट रूप से बताया जाना चाहिए कि साइबर सुरक्षा के संदर्भ में क्या अपेक्षित है, जैसे एन्क्रिप्शन मानक आदि.

डेटा एक्सैस सीमित करें

न्यूनतम विशेषाधिकार की अवधारणा का पालन करते हुए आपूर्तिकर्ताओं को केवल उतना ही एक्सैस प्रदान करें जितनी उन्हें अपने कार्य निष्पादित करने के लिए आवश्यकता है.

घटना प्रतिक्रिया संबंधी प्रोटोकॉल सेट अप करें

सुनिश्चित करें कि आपके प्रदाता जानते हैं कि सुरक्षा समस्याओं की रिपोर्ट कैसे करें और उन्हें किस तरह से संभालें, जो आपकी अपनी आईआर योजना के साथ काम करे.

आपूर्तिकर्ताओं का अद्यतन रिकॉर्ड रखें

सुनिश्चित करें कि आपके सभी तृतीय-पक्ष प्रदाताओं की सूची, उनके एक्सैस का स्तर, तथा उनके साथ आने वाले खतरे हमेशा अद्यतन रहें.

अपने कर्मचारियों को प्रशिक्षित करें

उन्हें बताएँ कि विक्रेताओं के साथ सही तरीके से कैसे व्यवहार करें और बाहरी स्रोतों से आने वाले खतरों को कैसे पहचानें.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

तृतीय पक्ष सुरक्षा प्रबंधन

क्या न करें!

यह मत मानिए कि आपूर्तिकर्ता डिफ़ॉल्ट रूप से सुरक्षित हैं

यहाँ तक कि जाने-माने लोगों में भी समस्याएँ हो सकती हैं. हमेशा जाँच-पड़ताल करें; सिर्फ़ भरोसा न करें.

बिना नियंत्रण के संवेदनशील डेटा साझा न करें

जब तक आप स्वयं न कहें, किसी को भी अपना संवेदनशील डेटा देखने न दें. अपने डेटा पर नज़र रखें और एन्क्रिप्शन का प्रयोग कर ट्रैक करें कि कौन इसे देख सकता है.

संविदात्मक सुरक्षा उपायों को न छोड़ें

अपनी संविदाओं में सुरक्षा संबंधी प्रावधान शामिल न करने से आप कानूनी और वित्तीय संकट में पड़ सकते हैं.

उल्लंघन की सूचना में अंतराल के बारे में न भूलें

सुनिश्चित करें कि अगर कोई उल्लंघन होता है, तो प्रदाता आपको तुरंत सूचित करें. बहुत से लोग ऐसा तब तक नहीं करते जब तक कि उन्हें ऐसा करना अनिवार्य न हो.

ऑफबोर्डिंग के चरण न भूलें

जब विक्रेता की संविदा समाप्त हो जाए, तो तुरंत एक्सैस बंद कर दें और सुनिश्चित करें कि डेटा सुरक्षित रूप से वापस कर दिया गया है या नष्ट कर दिया गया है.

वेंडर जोखिम में परिवर्तन को नज़रअंदाज़ न करें

किसी वेंडर का जोखिम प्रोफाइल समय के साथ बदल सकता है, अतः मूल्यांकन को ऐसी चीज न समझें जिसे आप एक बार ही करते हैं.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

नेटवर्क सुरक्षा

क्या करें

सुदृढ़ एक्सैस कंट्रोल लागू करें

महत्वपूर्ण प्रणालियों का एक्सैस सीमित करने के लिए सुदृढ़ एक्सैस कंट्रोल का प्रयोग करें. ऐसा करने के कई तरीके हैं, जिनमें भूमिका-आधारित एक्सैस, एमएफ़ए, और न्यूनतम विशेषाधिकार का सिद्धांत शामिल हैं.

नियमित सुरक्षा ऑडिट करें

एक मजबूत प्रतिक्रिया टीम बनाने के लिए कुशल कर्मियों को तकनीकी प्रतिक्रियाकर्ता आदि जैसी विशिष्ट भूमिकाएँ दें.

सिस्टम को अद्यतन रखें

पहले से पाई गई सुरक्षा संबंधी कमियों को ठीक करने के लिए ऑपरेटिंग सिस्टम, फर्मवेयर और एप्लिकेशन्स पर पैच और अपग्रेड का उपयोग करें.

ट्रांजिट और रेस्ट के दौरान डेटा एन्क्रिप्ट करें

संवेदनशील डेटा को स्थानांतरित या संग्रहित करते समय चोरी होने से बचाने के लिए HTTPS, VPN और TLS जैसे सुरक्षित प्रोटोकॉल का उपयोग किया जाता है.

कर्मचारियों को शिक्षित करें

अपने कर्मचारियों को सिखाएँ कि इंटरनेट का सुरक्षित उपयोग कैसे करें तथा फ़िशिंग और सोशल इंजीनियरिंग को कैसे पहचानें. अधिकांशतः वे ही सबसे कमज़ोर कड़ी होते हैं.

लॉग और ट्रैफ़िक चेक करें

लॉग देखने और समस्याओं को बदतर होने से पहले ही पता लगाने के लिए SIEM प्रौद्योगिकियों का उपयोग करें.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नेटवर्क सुरक्षा

क्या न करें!

डिफ़ॉल्ट क्रिडेंशियल्स का उपयोग न करें

डिफ़ॉल्ट उपयोगकर्ता नाम और पासवर्ड तुरंत बदलें क्योंकि हैकर्स आमतौर पर उनका उपयोग करते हैं.

किसी को भी अप्रतिबंधित एक्सैस न दें

हमलावर आसानी से उन सिस्टम में प्रवेश कर सकते हैं जिनमें खुले पोर्ट, असुरक्षित वाई-फाई या व्यापक अनुमतियां हों.

एंडपॉइंट सुरक्षा के बारे में न भूलें

असुरक्षित डिवाइस के ज़रिए कोई भी अंदर प्रवेश कर सकता है. एंटीवायरस, EDR और पैच मैनेजमेंट इंस्टॉल करें.

भौतिक सुरक्षा को न भूलें

सुनिश्चित करें कि राउटर, स्विच और सर्वर अवांछित एक्सैस से भौतिक रूप से सुरक्षित हैं.

यह न मानें कि क्लाउड सेवाएँ स्वचालित रूप से सुरक्षित हैं

आपको कभी भी यह नहीं मान लेना चाहिए कि क्लाउड सेवाएँ डिफ़ॉल्ट रूप से सुरक्षित हैं. उन्हें हमेशा सही तरीके से सेट अप करें और उन पर निगरानी रखें.

अपडेट में देरी न करें

पैच इंस्टॉल न करने से मशीनें पहले से ज्ञात हमलों के प्रति संवेदनशील हो जाती हैं.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

साइबर सुरक्षा हेतु प्रशिक्षण और जागरूकता

क्या करें

इसे एक-बारगी नहीं, बल्कि निरंतर जारी रखें

उभरते खतरों पर नजर रखने और अच्छी आदतें बनाए रखने के लिए नियमित सत्र आयोजित करें, जैसे महीने में एक बार या हर तीन महीने में एक बार.

वास्तविक स्थितियों का उपयोग करें

प्रशिक्षण को अधिक प्रभावी और अविस्मरणीय बनाने के लिए फ़िशिंग सिम्युलेशन, फर्जी उल्लंघन और व्यावहारिक गतिविधियाँ जोड़ें.

कर्मचारियों को नीतियों के बारे में सिखाएँ

सुनिश्चित करें कि आपके कर्मचारियों को डेटा, पासवर्ड, घर से काम करने और कठिनाइयों की रिपोर्टिंग से संबंधित नियमों की जानकारी हो.

ऐसा परिवेश बनाएँ जो सुरक्षा को सर्वोपरि रखे

अपने कर्मचारियों से कहें कि वे किसी भी अजीब व्यवहार की बिना किसी डर के रिपोर्ट करें. साइबर सुरक्षा के मामले में सिर्फ़ नियमों का पालन न करें.

सामग्री को नियमित रूप से अपडेट करें

सुनिश्चित करें कि आपकी प्रशिक्षण सामग्री एआई-जनित फ़िशिंग, डीपफेक या क्लाउड मिसकॉन्फ़िगरेशन जैसे उभरते खतरों के प्रति अद्यतन हो.

सुरक्षा उपकरणों के उपयोग को प्रोत्साहित करें

अपने कर्मचारियों को पासवर्ड मैनेजर, VPN, MFA और सुरक्षित फ़ाइल-शेयरिंग प्लेटफ़ॉर्म का सुरक्षित उपयोग करना सिखाएँ.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

साइबर सुरक्षा हेतु प्रशिक्षण और जागरूकता

क्या न करें!

गलती करने पर कर्मचारियों को दोष न दें

फ़िशिंग लिंक पर क्लिक करने या गलतियाँ करने पर लोगों को बुरा महसूस न कराएँ. सीखने और बेहतर बनने पर ध्यान केंद्रित करें.

ऐसा न सोचें कि एक ही युक्ति सभी के लिए उपयुक्त है

सामान्य प्रशिक्षण हमेशा कारगर नहीं होता. बदलाव इस बात पर निर्भर करता है कि आप कितना जोखिम उठाते हैं, आपका पेशा क्या है, और आप तकनीक में कितने कुशल हैं.

शब्दजाल का प्रयोग न करें

गैर-तकनीकी कर्मचारियों को अपने विचारों को बेहतर ढंग से समझने में सहायता करने के लिए सरल वाक्यांशों और चित्रों का उपयोग करें.

नए कर्मचारियों के बारे में न भूलें

सुनिश्चित करें कि प्रत्येक नया कर्मचारी सुरक्षा ऑनबोर्डिंग से गुजरे, ताकि वे सही दृष्टिकोण के साथ शुरुआत करें.

इसे चेकबॉक्स अभ्यास की तरह न समझें

प्रशिक्षण का उद्देश्य केवल लेखापरीक्षा मानदंडों को पूरा करना ही नहीं होना चाहिए; बल्कि इससे वास्तविक जागरूकता भी बढ़नी चाहिए.

फ़ॉलो अप करना न भूलें

लोगों को जो कुछ उन्होंने सीखा है उसे याद रखने में सहायता करने के लिए पूरे वर्ष न्यूज़लेटर, अनुस्मारक और सूक्ष्म प्रशिक्षण भेजें.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

एक्सैस कंट्रोल और विशेषाधिकार प्रबंधन

क्या करें

न्यूनतम विशेषाधिकार के सिद्धांत (POLP) का पालन करें

लोगों को सिर्फ़ उतना ही एक्सैस दें जितना उन्हें अपना कार्य करने के लिए आवश्यक है, इससे ज़्यादा कुछ नहीं. इससे हमले का प्रभाव कम हो जाता है और हमले की संभावना कम हो जाती है.

भूमिका-आधारित एक्सैस कंट्रोल (RBAC) का उपयोग करें

लोगों को उनकी भूमिकाओं के आधार पर मदें प्राप्त करने दें. इससे इसे चलाना आसान हो जाता है और यह सुनिश्चित होता है कि सभी विभाग समान नियमों का पालन करते हैं.

एक्सैस की समीक्षाओं को स्वचालित करें

यह सुनिश्चित करने के लिए नियमित जाँच की व्यवस्था करें कि लोगों को अभी भी दिए गए एक्सैस की आवश्यकता है.

जस्ट-इन-टाइम (JIT) विशेषाधिकार उन्नयन का उपयोग करें

लोगों को जब आवश्यक हो, तभी उच्चतर एक्सैस प्रदान करें और कार्य पूरा हो जाने पर इसे स्वचालित रूप से हटा लें.

एक्सैस की नियमित जाँच करें और उस पर नज़र रखें

लिखें कि किसने क्या, कब और कैसे एक्सेस किया. लॉग और अलर्ट का प्रयोग करके उन गतिविधियों और व्यवहारों का पता लगाएँ जो असामान्य और नियमों के विरुद्ध हैं.

केंद्रीकृत पहचान प्रबंधन

सभी सिस्टम पर पहचानों का ट्रैक रखने के लिए IAM टूल्स का प्रयोग करें. इससे चीज़ें स्पष्ट और समझने में आसान हो जाती हैं.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

एक्सैस कंट्रोल और विशेषाधिकार प्रबंधन

क्या न करें!

उपयोगकर्ताओं को व्यापक या स्थायी ऐडमिन एक्सैस न दें

उपयोगकर्ताओं को अनियंत्रित या दीर्घकालिक उन्नत विशेषाधिकार देना एक बड़ा सुरक्षा जोखिम है.

डिफ़ॉल्ट सेटिंग्स पर निर्भर न रहें

एक्सैस के लिए डिफ़ॉल्ट सेटिंग्स आमतौर पर बहुत ज़्यादा अनुमति देने वाली होती हैं. जाँच करें कि क्या वे आपकी सुरक्षा आवश्यकताओं को पूरा करती हैं.

एक्सैस की समीक्षा अवश्य करें

यदि आप अक्सर एक्सैस की जाँच नहीं करते हैं, तो आप सुरक्षा संबंधी कमियों को नजरअंदाज कर सकते हैं और विशेषाधिकार को घुसपैठ करने का मौका दे सकते हैं।

रद्द करने का इंतजार न करें

यदि किसी को अब एक्सैस की आवश्यकता नहीं है, तो उसे तुरंत वापस ले लें, विशेषतः यदि उनके पास विशिष्ट विशेषाधिकार हों.

निष्क्रिय खातों को नज़रअंदाज़ न करें

उन लोगों से एक्सैस वापस ले लें जिन्होंने कंपनी छोड़ दी है या नौकरी बदल दी है. उन खातों तक पहुँचना आसान है जिन्हें लोग याद नहीं रखते.

तृतीय-पक्ष संबंधी एक्सैस के बारे में न भूलें

विक्रेताओं और ठेकेदारों पर भी आंतरिक उपयोगकर्ताओं के समान ही कड़े नियंत्रण होने चाहिए.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

आस्ति प्रबंधन

क्या करें

केंद्रीकृत इनवेंटरी रखें

हार्डवेयर, सॉफ़्टवेयर, क्लाउड संसाधन और मोबाइल उपकरणों सहित अपनी सभी आस्तियों पर नज़र रखने के लिए एक ही सिस्टम या आस्ति प्रबंधन एप्लिकेशन का उपयोग करें. इस तरह आप उन सभी की देखरेख और प्रबंधन कर सकते हैं.

जोखिम और गंभीरता के आधार पर आस्तियों का वर्गीकरण करें

पता लगाएँ कि कौन सी आस्तियाँ कार्य के लिए आवश्यक हैं या उनमें निजी जानकारी शामिल है, और सुनिश्चित करें कि उन्हें सबसे पहले संरक्षित किया जाए.

स्वचालित खोज और अनुप्रवर्तन

नए संसाधनों को खोजने के लिए उपकरणों का उपयोग करें और तत्समय परिवर्तनों पर नज़र रखें ताकि आप कुछ भी न चूकें.

सुरक्षा उपकरणों का उपयोग करें

अपने आस्ति डेटा को SIEM, भेद्यता स्कैनर और पैच प्रबंधन प्रणालियों से कनेक्ट करें ताकि आपकी आस्तियों पर हमला होने से पहले उनकी सुरक्षा की जा सके.

मूल्यांकन में शैडो आईटी को शामिल करें

ऐसे डिवाइस और ऐप्स पर नज़र रखें जो अनुमोदित या प्रबंधित नहीं हैं और जो सुरक्षा नियंत्रणों को दरकिनार कर सकते हैं.

आस्तियों को स्पष्ट रूप से टैग और लेबल करें

प्रत्येक आस्ति को एक विशिष्ट आईडी दें ताकि आप आसानी से उस पर नज़र रख सकें, उसकी जाँच कर सकें और उसके जीवन चक्र का प्रबंधन कर सकें.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930

नाबार्ड

आस्ति प्रबंधन

क्या न करें!

एंड-ऑफ-लाइफ आस्तियों के बारे में न भूलें

ऐसी आस्तियाँ जो अब समर्थित नहीं हैं या समाप्त की जा चुकी हैं, वे तब भी खतरनाक हो सकती हैं यदि उनका उचित तरीके से निस्तारण नहीं किया या उन्हें मिटाया नहीं गया.

मैन्युअल रूप से ट्रैक न रखें

स्प्रेडशीट और एड-हॉक सूचियों में गलतियाँ करना आसान है, और ये जल्दी पुरानी हो जाती हैं. जब भी हो सके, इन्हें स्वचालित करें.

आस्ति अपडेट में विलंब न करें

हैकर्स उन डिवाइसों पर हमला करना पसंद करते हैं जिनमें पुराना फर्मवेयर हो या पैच न किया गया हो.

मोबाइल और दूरस्थ आस्तियों के बारे में न भूलें

आपकी आस्तियों की सूची में लैपटॉप, फोन और क्लाउड इंस्टैंस शामिल होने चाहिए, विशेषतः इसलिए क्योंकि अधिक लोग घर से काम कर रहे हैं.

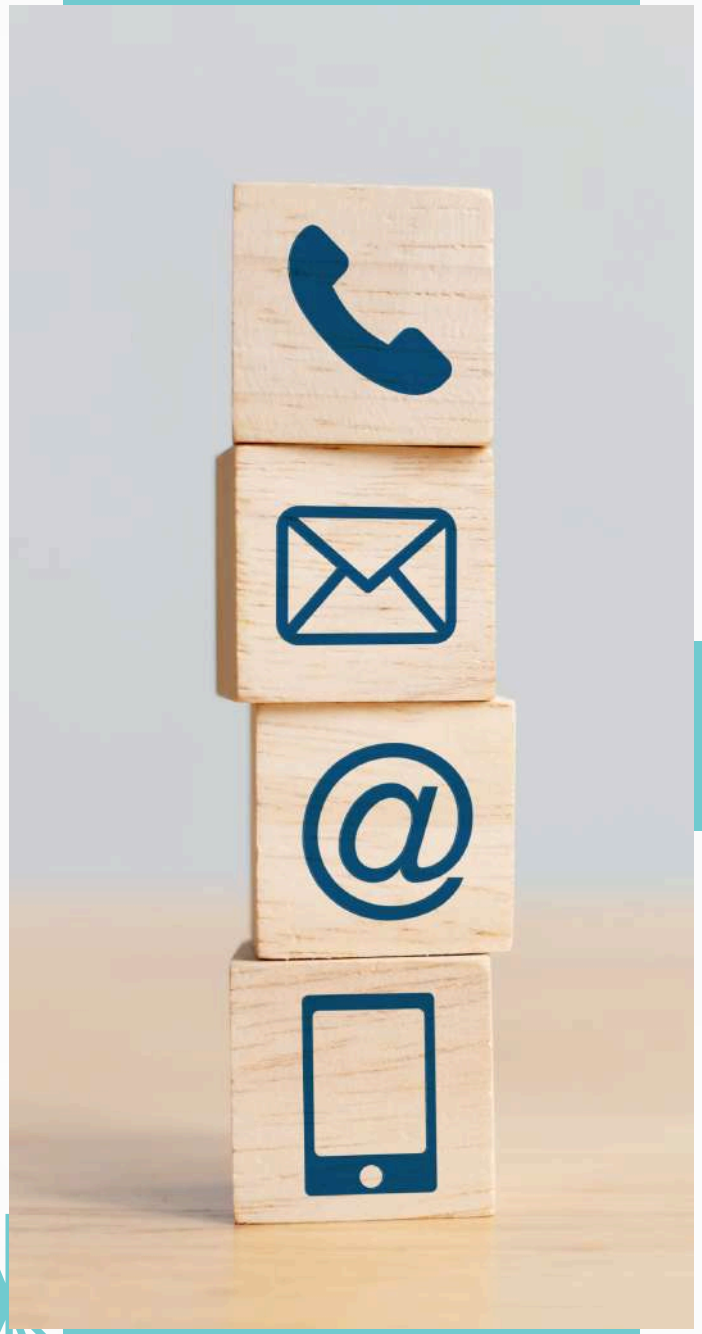
अप्रबंधित डिवाइसों को नेटवर्क से कनेक्ट न होने दें

प्रत्येक उपकरण की जाँच की जानी चाहिए, उस पर नजर रखी जानी चाहिए तथा नियमों का पालन किया जाना चाहिए.

सभी आस्तियों के साथ समान व्यवहार न करें

सभी आस्तियों को समान स्तर की सुरक्षा की आवश्यकता नहीं होती. अपने संसाधनों को वहाँ लगाएँ जहाँ वे सबसे अधिक उपयोगी हों.

राष्ट्रीय साइबर अपराध हेल्पलाइन नंबर 1930



अधिक जानकारी के लिए

हमसे संपर्क करें

csite@nabard.org

पर्यवेक्षण विभाग, चौथा तल,
नाबार्ड प्रधान कार्यालय'

022-2653 9028/ 9250/ 9484/ 9163

नाबार्ड

2025

अंतर्राष्ट्रीय सहकारिता वर्ष

नाबार्ड

नाबार्ड शब्द संपदा वर्ष 2025

/nabardonline