वनकार्ड मोबाइल एप्लिकेशन के सुरक्षित उपयोग हेतु दिशा-निर्देश

04 सितंबर, **2026** को अपडेट किया गया

इस दस्तावेज़ में "वनकार्ड" मोबाइल एप्लिकेशन (“**ऐप**”) की सेवाओं का लाभ उठाने और उसके सुरक्षित उपयोग हेतु सामान्य दिशा-निर्देश दिए गए हैं, जिन्हें FPL टेक्नोलॉजीज़ प्राइवेट लिमिटेड और इसमें शामिल इसकी सहयोगी कंपनियाँ ('**कंपनी**') संचालित करती हैं और उनका प्रबंधन करती है।

क्या करें

- ऐप को हमेशा किसी सुरक्षित स्टोर (गूगल प्ले स्टोर या IOS स्टोर) से ही डाउनलोड करें।
- अपने क्रेडिट कार्ड के स्टेटमेंट की समय-समय पर जांच करें, ताकि पक्का हो सके कि आपके कार्ड से होने वाला हर लेनदेन सही है या नहीं।
- अपना फ़ोन बदलते, बेचते, किसी को देते या मरम्मत के लिए देते समय, पक्का करें कि ऐप अनइंस्टॉल कर दिया गया हो, साथ ही टेम्परररी फ़ाइलें, ब्राउज़िंग हिस्ट्री और कैश भी डिलीट कर दिया गया हो।
- अगर आपके पास कोई संदिग्ध ई-मेल आता है और आप अनजाने में उसे अपनी निजी या फ़ाइनेंशियल जानकारी दे देते हैं, तो help@getonecard.app पर तुरंत इसकी सूचना दें।
- धोखाधड़ी की शिकायत हमेशा दर्ज कराएं। अगर आपने ऐसे किसी संदिग्ध ई-मेल का जवाब दिया है, तो help@getonecard.app पर तुरंत इसकी सूचना दें।
- अपना ऐप पिन/पासवर्ड सिर्फ़ इसके लिए निर्धारित जगह पर डालें। हर 90 (नब्बे) दिनों में कम से कम एक बार अपना ऐप पिन/पासवर्ड बदलें।
- आप अपने मोबाइल डिवाइस में लॉग-इन करने के लिए फ़िंगरप्रिंट ऑथेंटिकेशन भी चालू कर सकते हैं।
- मल्टी-फ़ैक्टर ऑथेंटिकेशन का इस्तेमाल करें, क्योंकि इससे पासवर्ड के अलावा भी सुरक्षा की एक अतिरिक्त परत जुड़ जाती है।
- ऐप का इस्तेमाल पूरा होने के बाद उसे बंद करना न भूलें।
- जब भी कोई नया अपडेट आए, तो अपने मोबाइल डिवाइस पर ऐप और मोबाइल डिवाइस के सॉफ़्टवेयर को नियमित रूप से अपडेट करें।
- आप ऐप के 'माई कंट्रोल्स' वाले सेक्शन में जाकर ऑनलाइन ट्रांज़ैक्शन, POS भुगतान, कॉन्टैक्टलेस/टैप टू पे और BharatQR ट्रांजैक्शन की लिमिट सेट कर सकते हैं। यह सलाह

दी जाती है कि ऊपर बताए गए हर तरह के ट्रांजैक्शन के लिए लिमिट को कम-से-कम रखें। ज़रूरत पड़ने पर आप ऐप के ज़रिए इस लिमिट को बदल भी सकते हैं।

- आप ऐप के 'माई कंट्रोल्स' वाले सेक्शन में जाकर ऑनलाइन ट्रांज़ैक्शन, POS भुगतान, कॉन्टैक्टलेस/टैप टू पे और BharatQR ट्रांजैक्शन में से किसी को भी चालू या बंद कर सकते हैं।

क्या नहीं करें

- आपके ऐप का पिन / पासवर्ड वो नहीं होना चाहिए, जो आपने दूसरे ऐप्स के लिए रखा है।
- अपने ऐप का पिन / पासवर्ड किसी को नहीं बताएँ, क्योंकि इससे सुरक्षा का खतरा हो सकता है।
- ऐसे ऐप्स डाउनलोड करने से बचें जो आपके फोन का रिमोट एक्सेस ले सके या आपके ऐप की स्क्रीन को रिकॉर्ड कर सके।
- अपने मोबाइल डिवाइस पर पासवर्ड सेव न करें।
- ऐप का इस्तेमाल करते समय असुरक्षित वाई-फ़ाई नेटवर्क का इस्तेमाल करने से बचें।
- किसी भी संदिग्ध ई-मेल, वेबसाइट, सोशल मीडिया नेटवर्क, टेक्स्ट मैसेज या फ़ोन कॉल के ज़रिए ऐप से जुड़ी अपनी कोई भी गोपनीय जानकारी साझा न करें।
- कंपनी कभी भी किसी उपयोगकर्ता या ग्राहक से कोई दूसरा एप्लिकेशन इंस्टॉल करने या अपनी स्क्रीन शेयर करने के लिए नहीं कहती है। कंपनी कभी भी कार्ड नंबर या CVV जैसी ग्राहक की जानकारी पाने के लिए ई-मेल/SMS नहीं भेजती है या फ़ोन कॉल नहीं करती है। अगर आपको ऐसा कोई ई-मेल मिले जो कंपनी की तरफ़ से भेजा गया हो, तो कृपया help@getonecard.app पर ई-मेल करके तुरंत इसकी सूचना दें।