

भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या 1805
जिसका उत्तर 10 दिसंबर, 2025 को दिया जाना है।
19 अग्रहायण, 1947 (शक)

ज़ोहो-आधारित ईमेल माइग्रेशन की लागत और निरीक्षण

1805. श्री अभिषेक बनर्जी:

क्या इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री यह बताने की कृपा करेंगे कि:

- (क) 30 सितम्बर 2025 तक मंत्रालय-वार केन्द्र सरकार के कितने कर्मचारियों के आधिकारिक ईमेल खाते ज़ोहो प्लेटफार्म पर स्थानांतरित कर दिए गए हैं;
- (ख) वित्तीय वर्ष 2023-24 से सॉफ्टवेयर लाइसेंस, बनियादी ढांचे और प्रशिक्षण सहित स्थानांतरण प्रक्रिया पर किया गया कुल व्यय और वार्षिक आवर्ती लागत कितना है; और
- (ग) क्या डेटा की उपलब्धता, सुरक्षा ऑडिट अधिकार और रोलबैक विकल्प सुनिश्चित करने के लिए सेवा स्तर समझौते (एसएलए) किए गए हैं और यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से (ग): सरकार अपने मंत्रालयों और विभागों के लिए एक मजबूत, संप्रभु और सुरक्षित आधिकारिक ई-मेल प्रणाली के महत्व को स्वीकार करती है। तदनुसार, सरकार अधिदेशित करती है कि आधिकारिक संचार के लिए केवल राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) द्वारा प्रदान की जाने वाली ई-मेल सेवाओं का उपयोग किया जाएगा।

इसे सुनिश्चित करने के लिए, सरकार ने एनआईसी के माध्यम से एक मास्टर सिस्टम इंटीग्रेटर (एमएसआई) - मैसर्स ज़ोहो का चयन किया है, जो सभी सरकारी उपयोगकर्ताओं का समर्थन करने में सक्षम क्लाउड-आधारित ईमेल समाधान है।

यह मॉडल पेशेवर अपग्रेड, मौजूदा खातों का निर्बाध प्रवासन और वर्ड प्रोसेसर, स्प्रेडशीट और प्रेजेंटेशन सॉफ्टवेयर जैसे आधुनिक कार्यालय उत्पादकता उपकरणों का एकीकरण सुनिश्चित करता है।

अनुबंध में जहां आवश्यक हो, गारंटीकृत निरंतरता और रोलबैक विकल्पों के साथ-साथ भागीदारी के दौरान उत्पन्न सभी डेटा और आईपी के सरकारी स्वामित्व को सुनिश्चित करने वाले प्रावधान शामिल हैं।

महत्वपूर्ण सरकारी डेटा की सुरक्षा के लिए ई-मेल प्लेटफॉर्म की सुरक्षा संरचना को सख्ती से परिभाषित किया गया है। समाधान में यह अनिवार्य किया गया है कि सभी ईमेल डेटा को आरएसए 256 और टीएलएस 1.3 मानकों का उपयोग करके एंड-टू-एंड एन्क्रिप्शन के लिए विशिष्ट आवश्यकताओं के साथ रेस्ट और ट्रांज़िट दोनों में एन्क्रिप्ट किया जाए।

सेवा प्रदाता से अपेक्षित है कि वह आईएसओ 27001, आईएसओ/आईईसी 27017 और आईएसओ 27018 सहित कठोर नियंत्रण मानकों और अधिप्रमाणनों का अनुपालन करे।

प्रमुख तकनीकी सुरक्षा आवश्यकताओं में शामिल हैं:

- सभी प्रोटोकॉल (वेब, आईएमएपी, एसएमटीपी, पीओपी और कैलेंडर) में उपयोगकर्ता पहचान के लिए बहु-कारक प्रमाणीकरण (एमएफ़ए) का कार्यान्वयन
- जियो-फेंसिंग और आईपी-आधारित प्रतिबंधों का अनुप्रयोग, और
- ईमेल स्पूफिंग से निपटने के लिए उद्योग मानकों और नीतियों का उपयोग

सेवा को उच्च विश्वसनीयता के लिए डिज़ाइन किया गया है, जिसमें 24x7x365 के आधार पर कम से कम 99.9% की सेवा उपलब्धता अपटाइम को अनिवार्य किया गया है।

समाधान में कैलेंडर प्रबंधन, कार्य शेड्यूलिंग और सुरक्षित फ़ाइल साझाकरण जैसी एकीकृत सुविधाओं के साथ विभिन्न सदस्यता योजनाएं (मानक, व्यवसाय, उद्यम) शामिल हैं।

व्यवसाय की निरंतरता सुनिश्चित करने के लिए, सेवा प्रदाता को आकस्मिकताओं के दौरान डेटा हानि को कम करने के लिए सख्त वसूली समय उद्देश्यों (आरटीओ) और रिकवरी प्वाइंट उद्देश्यों (आरपीओ) के साथ कम से कम 500 किलोमीटर की दूरी पर विभिन्न भूकंपीय क्षेत्रों में आपदा रिकवरी स्थलों को बनाए रखना आवश्यक है।

जोहो प्लेटफॉर्म पर माइग्रेट किए गए खातों की संख्या लगभग 12.68 लाख है जिसमें केंद्र सरकार के 7.45 लाख कर्मचारी शामिल हैं।
