ACCCF / अनुप्रयुक्त ज्ञान पुस्तकालय

खंड ०८

सत्यापनयोग्य सामग्री और संदेश की सुरक्षा

स्पेनिश संस्करण · 2026

ईमेल, प्रकाशनों और सोशल मीडिया के प्रमाणन की पुस्तिका

EML, हेडर, URL, फ़ाइलें, प्रकाशन, ट्रेसेबिलिटी और प्रस्तुति

किसी संदेश या प्रकाशन के गायब होने से पहले उसकी समीक्षा संभव बनाने वाली सामग्री सुरक्षित रखें; स्क्रीनशॉट को उसका स्रोत और स्क्रीन पर दिखने वाली तिथि को उसकी उत्पत्ति का प्रमाण न मानें।

वकील, विशेषज्ञ, अनुपालन एवं संचार उत्तरदायित्व, शीर्षकताओं तथा उन लोगों के लिए जिन्हें कोई ईमेल, प्रकाशन या ऑनलाइन वार्तालाप सुरक्षित रखना हो। नोटरी, विशेषज्ञ या प्रशासनिक प्रमाणन क्षेत्राधिकार और प्रक्रिया पर निर्भर करता है।

संपादकीय समन्वय: जोसान लैगुन · अमेरिकी साइबर सुरक्षा और फोरेंसिक कम्प्यूटिंग परिषद

सामान्य तकनीकी मार्गदर्शिका और खुली शैक्षिक सामग्री। यह कानूनी सलाह, विशेषज्ञ राय या बिना प्राधिकरण के सिस्टम तक पहुँचने के निर्देश नहीं है। उदाहरण और डेटा काल्पनिक हैं; आकृतियाँ संपादकीय पुनर्निर्माण हैं।

सामग्री

दिखाई देने वाला पृष्ठांकन PDF संस्करण से संबंधित है। Word दस्तावेज़ खोलते समय इस अनुक्रमणिका को अद्यतन कर सकता है; शीर्षक आंतरिक नेविगेशन बनाए रखते हैं।

प्रस्तावना: बदलने से पहले संरक्षित करें 3

अध्याय 1. दायरा और तैयारी 3

- **1.1 किस दावे को सिद्ध करना आवश्यक है** 3
- **1.2 कैप्चर का वातावरण तैयार करना** 4

अध्याय 2. पूरा संदेश 4

- **2.1 EML: मुख्य भाग, हेडर और संलग्नक** 4
- **2.2 पुनः भेजना, डाउनलोड करना और रूपांतरण** 4
- **2.3 संलग्नक और तीसरे पक्ष द्वारा डिलीवरी** 5

अध्याय 3. चैनल का प्रमाणीकरण 5

- **3.1 Received हेडर और परिवहन** 5
- **3.2 DKIM, SPF और DMARC** 5
- **3.3 तिथि, Message-ID और सामग्री** 6

अध्याय 4. फ़ाइलें, URL और प्रकाशन 7

- **4.1 किसी URL का पूर्ण रिकॉर्ड** 7
- **4.2 प्रकाशन, थ्रेड और मल्टीमीडिया** 7
- **4.3 वेब संग्रह और तीसरे पक्ष की तिथियाँ** 7

अध्याय 5. दस्तावेज़ित संरक्षण और प्रमाणन 8

- **5.1 अधिग्रहण-अभिलेख** 8
- **5.2 कस्टडी और पहुँच नियंत्रण** 8
- **5.3 विशेषज्ञ, नोटरी या प्रशासनिक प्रमाणन** 9

अध्याय 6. हटाना, शिकायत और मीडिया-क्षति 9

- **6.1 निकालने से पहले संरक्षित करें** 9
- **6.2 क्षति और पहुँच** 9
- **6.3 एकीकृत मामला** 9

परिशिष्ट A. संरक्षण प्रारूप 10

- **A.1 ईमेल-अभिलेख** 10
- **A.2 प्रकाशन रिकॉर्ड** 10
- **A.3 ऑब्जेक्ट मैनिफ़ेस्ट** 10
- **A.4 हटाने के अनुरोध का रिकॉर्ड** 10

परिशिष्ट B. कानूनी ढाँचा और अंतिम सूची 11

प्रस्तावना: बदलने से पहले संरक्षित करें

एक प्रकाशन संपादित हो सकता है, खाता बंद हो सकता है, संलग्न फ़ाइल बदली जा सकती है और लिंक काम करना बंद कर सकता है। संरक्षण का उद्देश्य यह अभिलिखित करना है कि किस समय क्या मौजूद था, कहाँ था, कैसे प्राप्त हुआ और कौन-सा रूप सुरक्षित रहा। स्क्रीनशॉट किसी अंश को दिखा सकता है, लेकिन समीक्षा के लिए पूरा ऑब्जेक्ट और उसका संदर्भ चाहिए: URL, खाता, तिथि, समय क्षेत्र, फ़ाइलें, उत्तर, मेटाडेटा और अधिग्रहण प्रक्रिया।

ईमेल इसका स्पष्ट उदाहरण है। यदि संदेश की केवल छवि सुरक्षित रखी जाए, तो हेडर, संरचना और संलग्नक खो जाते हैं। यदि केवल संलग्नक सुरक्षित रखा जाए, तो यह बताने वाला मुख्य पाठ खो जाता है कि उसमें क्या है और कुछ मामलों में उसे सत्यापित करने वाला हैश भी। EML इन घटकों को एक साथ रखता है और उनमें संबंध स्थापित करने देता है। इससे यह सिद्ध नहीं होता कि सभी दावे सत्य हैं या मुख्य भाग किसी विशेष व्यक्ति ने लिखा।

यहाँ “प्रमाणन” शब्द का अर्थ दस्तावेज़ित प्रक्रिया है, सार्वभौमिक गारंटी नहीं। नोटरी कार्यवाही, विशेषज्ञ परीक्षण, संरक्षण प्रमाणपत्र और साक्षी के समक्ष लिए गए कैप्चर के कार्य और प्रभाव अलग-अलग हो सकते हैं। संरक्षण करने वाले व्यक्ति को बताना चाहिए कि उसने क्या किया और वह क्या सिद्ध कर सकता है; अधूरे स्रोत को ढकने के लिए अनावश्यक औपचारिकता नहीं जोड़नी चाहिए।

> **स्वर्ण नियम**
> सामग्री और संदर्भ दोनों एक साथ सुरक्षित रखें। बिना URL और तिथि वाली किसी प्रकाशन की स्पष्ट छवि उपयोगी संदर्भ है, ऑब्जेक्ट का पूर्ण पुनर्निर्माण नहीं।

अध्याय 1. दायरा और तैयारी

1.1 किस दावे को सिद्ध करना आवश्यक है

यह सिद्ध करना एक ही बात नहीं है कि कोई प्रकाशन मौजूद था, किसी खाते ने उसे प्रकाशित किया, किसी व्यक्ति ने उसे लिखा, वह सार्वजनिक रूप से उपलब्ध था, उसमें धमकी थी, या किसी विशेष फ़ाइल की डिलीवरी हुई। दावा स्रोत तय करता है: दिखाई देने वाला प्रकाशन, निर्यात, EML, प्लेटफ़ॉर्म रिकॉर्ड, प्राप्तकर्ता, प्रशासक या साक्षी। यदि केवल किसी तिथि पर अस्तित्व सिद्ध करना है, तो विश्लेषण को लेखकत्व तक न बढ़ाएँ।

अवधि, खाते, URL, मुख्य शब्द, प्रतिभागी, सामग्री के प्रकार और तीसरे पक्ष के डेटा का दायरा तय किया जाता है। यह भी तय होता है कि संरक्षण का उपयोग शिकायत, हटाने, प्रक्रिया, आंतरिक जाँच या अभिलेखीय प्रमाण के लिए होगा। संरक्षण की तात्कालिकता न तो अधिकार की आवश्यकता समाप्त करती है और न तीसरे पक्षों की सुरक्षा।

उद्देश्य	प्राथमिक स्रोत	साबित की जाने वाली सीमा
प्रकाशन का अस्तित्व	URL, सामग्री, पृष्ठ और दस्तावेज़ित संरक्षण।	इससे सीधे लेखकत्व या खाते की संपूर्णता सिद्ध नहीं होती।
ईमेल की सामग्री	मुख्य भाग, हेडर और संलग्नक सहित EML।	इससे पाठ की सत्यता सिद्ध नहीं होती।
फ़ाइल की डिलीवरी	संलग्नक, मुख्य भाग, हैश, डाउनलोड और मानिफ़ेस्ट।	यह खाते प्रणाली के फ़ैसलों को प्रमाणित नहीं करता है।
सार्वजनिक पहुँच	दृश्यता, पैराफ़, लिंक और पहुँच का प्रमाण।	यह वास्तविक पाठकों की संख्या के बराबर नहीं है।
लेखकत्व का नियंत्रण	खाता, सत्र, डिवाइस और समय।	दिखाई देने वाला नाम व्यक्ति को पहचान नहीं करता है।
क्रम	गतिविधि, समय क्षेत्र, उत्तर, संपादन और समय।	केवल एक स्क्रीनशॉट पूरे इतिहास को क्रम नहीं बताता।

1.2 कैप्चर का वातावरण तैयार करना

अधिकृत डिवाइस और खाते का उपयोग करें, तिथि और समय क्षेत्र दर्ज रखें, ज्ञात ब्राउज़र तथा नियंत्रित स्टोरेज का उपयोग करें। ऐसे व्यक्तिगत खाते से लॉग इन न करें जिससे प्रमाण में अनावश्यक डेटा जुड़े। प्रकाशन से आवश्यकता से अधिक संवाद न करें: उत्तर देने, शिकायत करने या साझा करने से उसकी पहुँच बदल सकती है और लेखक को सूचना मिल सकती है।

मूल, कार्य-प्रति, कैप्चर, निर्यात, रिकॉर्ड और मैनिफ़ेस्ट के लिए फ़ोल्डर तैयार करें। संभावित अवैध या हानिकारक सामग्री पूरी टीम में न बाँटें। उसकी मौजूदगी दस्तावेज़ित करें और प्रतिबंधित चैनल से सौंपें। यदि किसी व्यक्ति को जोखिम है, तो प्राथमिकता उसकी सुरक्षा और सक्षम चैनलों से संपर्क है, अतिरिक्त तकनीकी प्रदर्शन नहीं।

> **पूर्व निर्णय**
> यदि प्रकाशन गायब हो सकता है और उसे सुरक्षित रखने का अधिकार है, तो पहले ऑब्जेक्ट और उसका संदर्भ दर्ज करें। इसके बाद हटाने या समीक्षा का अनुरोध करें। संरक्षण से पहले हटा देने पर केवल स्रोत-विहीन दावा रह सकता है।

अध्याय 2. पूरा संदेश

2.1 EML: मुख्य भाग, हेडर और संलग्नक

RFC 5322 इंटरनेट संदेशों के प्रारूप का वर्णन करता है, जिसमें हेडर फ़ील्ड और मुख्य भाग होते हैं। EML ईमेल के उन घटकों और उसमें मौजूद संलग्नकों सहित एक प्रतिनिधित्व सुरक्षित रखने देता है। यह दस्तावेज़ित करें कि वह कैसे प्राप्त हुआ: क्लाइंट से निर्यात, सर्वर से डाउनलोड या किसी अन्य व्यक्ति द्वारा डिलीवरी। उद्गम व्याख्या बदलता है; उसे ज्ञात फ़ाइल एक्सटेंशन के आड़ में न छिपाएँ।[1]

ऐसे उपकरणों से खोलने से पहले फ़ाइल सुरक्षित रखें जो उसे बदल सकते हैं। EML और प्रत्येक संलग्नक का अलग हैश निकालें और उसे मैनिफ़ेस्ट में संबद्ध करें। मुख्य भाग में किसी फ़ाइल का एल्गोरिदम और मान दिया हो सकता है: उसे जाँचें, किसी अलग नोट में कॉपी करके न छोड़ें। अंतर होने पर पहली डिलीवरी सुरक्षित रखें और स्पष्टीकरण माँगें।

2.2 पुनः भेजना, डाउनलोड करना और रूपांतरण

ईमेल पुनः भेजने से हेडर जुड़ सकते हैं और संदेश व फ़ाइलों का संबंध बदल सकता है। PDF में प्रिंट करने से दृश्य सुरक्षित रहता है, संरचना नहीं। वेबमेल से डाउनलोड करने पर अलग प्रारूप मिल सकते हैं। प्रत्येक कार्रवाई दर्ज करें और सभी संस्करण सुरक्षित रखें; पुनः भेजे गए संदेश को आवश्यक रूप से मूल संदेश न मानें।

पुनः भेजा गया संदेश उस व्यक्ति द्वारा उस तिथि पर प्राप्त सामग्री का उपयोगी प्रमाण हो सकता है, लेकिन उसकी पिछली सामग्री का विश्लेषण हेडर और पूरक स्रोतों से करें। यदि फ़ाइल की डिलीवरी सिद्ध करनी है, तो प्रदाता से प्राप्त मूल EML पुनः भेजे गए संदेश के स्क्रीनशॉट से बेहतर है। यदि उपलब्ध न हो, तो सीमा बताएँ और दूसरे मेलबॉक्स या सर्वर में संदेश खोजें।

प्रतिनिधित्व	क्या सुरक्षित रहता है	किस पूरक की आवश्यकता है
मूल EML	उपलब्ध मुख्य भाग, हेडर और संलग्नक।	उद्गम और सामग्री सत्यापन।
पुनः भेजा गया EML	नई डिलीवरी और प्रस्तुत की गई पिछली सामग्री।	पुनः भेजने का इतिहास और पिछला उद्गम।
इनले PDF	लेआउट और पठनीय पाठ।	हेडर, संलग्नक और संरचना।
स्क्रीनशॉट	स्क्रीन पर दिखाया गया अंश।	URL, खाता, तिथि, संदर्भ और फ़ाइल।
केवल संलग्नक	किसी फ़ाइल की प्रति।	संदर्भ, विवरण, संबंध और प्रासंगिकता।

[1] RFC Editor. RFC 5322, Internet Message Format: संदेश संरचना, हेडर और मुख्य भाग। यह ईमेल सुरक्षित रखने और समझने का तकनीकी संदर्भ है, मानव पहचान का स्वचालित प्रमाण नहीं। आधिकारिक ऑनलाइन स्रोत

2.3 संलग्नक और तीसरे पक्ष द्वारा डिलीवरी

संलग्नक को सुरक्षित रखने से पहले पढ़ने में आसान बनाने के लिए उसे संपादित या रूपांतरित न करें। हैश निकालें, घोषित मान से मिलान करें तथा खोलने और कवरेज का रिकॉर्ड रखें। यदि CSV खुलता है लेकिन उसका डेटा डिक्शनरी नहीं है, तो फ़ील्ड का अर्थ पूछें। हैश यह सिद्ध नहीं करता कि पंक्तियाँ पूरी या सत्य हैं; यह तुलना की गई दो वस्तुओं की समानता सिद्ध करता है।

> **काल्पनिक मामला**
> कोई प्रदाता CSV और PDF देता है तथा ईमेल के मुख्य भाग में प्रत्येक का हैश देता है। CSV का हैश मेल खाता है, PDF का नहीं। सब कुछ सुरक्षित रखें, PDF की नई डिलीवरी माँगें और दर्ज करें कि CSV घोषित मान से मेल खाता है, बिना यह दावा किए कि प्रदाता की सामग्री पूरी है। दूसरी डिलीवरी को दूसरा पहचानकर्ता दें; वह पहली का स्थान नहीं लेती।



चित्र 1. EML, संलग्नक और विवरण: संबंधित ऑब्जेक्ट। प्रत्येक अखंडता किसी अलग ऑब्जेक्ट से संबंधित है। संपादकीय पुनर्रूपण; वास्तविक प्रमाण नहीं।

अध्याय 3. चैनल का प्रमाणीकरण

3.1 Received हेडर और परिवहन

Received फ़ील्ड सर्वरों, तिथियों और परिवहन डेटा का घोषित क्रम देते हैं। उन्हें संदेश संरचना के निर्धारित क्रम में जाँचें, यह न मानें कि सभी आवश्यक रूप से विश्वसनीय हैं या पहला दिखने वाला फ़ील्ड मानव स्रोत से जुड़ा है। कुछ फ़ील्ड मध्यवर्ती सिस्टम जोड़ सकते हैं। विश्लेषण में सर्वर, समय, डोमेन और अन्य प्रमाणीकरण परिणामों की तुलना करें।

दिखने वाला From पता प्रमाणित डोमेन या भेजने वाले सर्वर से मेल नहीं खा सकता। किसी हेडर की IP बुनियादी ढाँचे की पहचान करा सकती है, व्यक्ति की नहीं। तिथि अलग-अलग घड़ियों पर निर्भर कर सकती है। विश्लेषण किसी जटिल हेडर को जादुई प्रमाण नहीं बनाता; यह बताता है कि कौन-से घटक सत्यापनयोग्य हैं और कौन-से विश्वास पर निर्भर हैं।

3.2 DKIM, SPF और DMARC

DKIM क्रिप्टोग्राफ़िक हस्ताक्षर के माध्यम से डोमेन को संदेश से जोड़ता है और हस्ताक्षरित घटकों के सत्यापन की सुविधा देता है। SPF प्रोटोकॉल के संदर्भ में बताता है कि डोमेन के लिए कौन-से होस्ट अधिकृत हैं; DMARC डोमेन संरेखण और नीति देता है। ये तंत्र चैनल

और डोमेन के मूल्यांकन में मदद करते हैं, लेकिन यह सिद्ध नहीं करते कि पाठ किसने लिखा या वह सत्य है। विफलता होने पर पुनः भेजने, कॉन्फ़िगरेशन या रूपांतरणों की समीक्षा भी आवश्यक हो सकती है।[2][3]

रिपोर्ट में उपलब्ध होने पर डोमेन, सेलेक्टर, हस्ताक्षरित फ़ील्ड, परिणाम, तिथि और क्वेरी स्रोत दर्ज करें। “DKIM pass” को व्यक्तिगत पहचान की तरह लिखना पर्याप्त नहीं है। “SPF fail” भी अपने आप दुर्भावनापूर्ण स्पूफ़िंग सिद्ध नहीं करता: मार्ग और कॉन्फ़िगरेशन जाँचें। तकनीकी विश्लेषण में मूल संदेश सुरक्षित रखें ताकि दूसरा व्यक्ति उसे जाँच सके।

3.3 तिथि, Message-ID और सामग्री

Message-ID संदेशों और सिस्टम को संबद्ध करने में मदद कर सकता है, लेकिन उसकी अद्वितीयता और संरचना उसे बनाने वाले सिस्टम पर निर्भर है। तिथियों को उनके समय क्षेत्र सहित यथावत सुरक्षित रखें और सर्वर रिकॉर्ड तथा प्राप्ति की घटनाओं से तुलना करें। डाउनलोड की तिथि भेजने की तिथि नहीं होती। संलग्न फ़ाइल की तिथि एक अलग परत है।

पथ	क्या सत्यापित किया जा सकता है	क्या निष्कर्ष नहीं निकलता
प्रमाणीकृत डोमेन	हस्ताक्षर, संरेखण और पब्लिक कॉन्फ़िगरेशन	किसी व्यक्ति ने संदेश लिखा।
संदेश की तिथि	तुलनात्मक हेडर और रिकॉर्ड।	पाठ उसी क्षण बनाया गया था।
प्राप्ति संदेश	मेलबॉक्स, EML और संदेश रिकॉर्ड।	व्यक्ति ने उसे पढ़ा या समझा।
सामग्री सत्य है	पाचित घटना के स्वतंत्र खाते।	DKIM या हेडर घटना को सिद्ध करता है।
सुरक्षा-सम्झौता हुआ खाता।	सत्र, पुनर्प्राप्ति और असामान्य गतिविधि।	सिर्फ़ जली पता होना चोरी सिद्ध करता है।

पढ़ने का नियम

हेडर का विश्लेषण परिवहन और डोमेन के प्रमाण के रूप में करें, व्यक्ति की स्वीकृति के रूप में नहीं। लेखकत्व के लिए अतिरिक्त पुष्टि आवश्यक है।



चित्र 2. हेडर पढ़ें बिना उन्हें मानव पहचान में बदलें। परिवहन, डोमेन और सामग्री के संकेत। संपादकीय पुनर्संरेखण; वास्तविक प्रमाण नहीं।

[2] RFC Editor. RFC 6376, DomainKeys Identified Mail (DKIM) Signatures: डोमेन का उत्तरदायित्व और हस्ताक्षरित घटकों का क्रिप्टोग्राफ़िक सत्यापन। यह अकेले यह सिद्ध नहीं करता कि पाठ किसने लिखा या सामग्री सत्य है। आधिकारिक ऑनलाइन स्रोत

[3] RFC Editor. RFC 8616 और तकनीकी संदर्भ SPF RFC7208, DKIM RFC6376 तथा DMARC RFC7489: होस्ट अधिकार, डोमेन हस्ताक्षर, संरेखण और नीति। ये चैनल के मूल्यांकन में मदद करते हैं; अकेले मानव पहचान या सामग्री की सत्यता सिद्ध नहीं करते। आधिकारिक ऑनलाइन स्रोत

अध्याय 4. फ़ाइलें, URL और प्रकाशन

4.1 किसी URL का पूर्ण रिकॉर्ड

पूरा URL, पैरामीटर, डोमेन, तिथि और समय क्षेत्र, दिखने वाला खाता, पहुँच का प्रकार, भूमिका, भाषा, ब्राउज़र संस्करण और पृष्ठ की स्थिति सुरक्षित रखें। रीडायरेक्ट, लॉग इन, भौगोलिक प्रतिबंध या त्रुटि दर्ज करें। URL का पता बदले बिना उसकी सामग्री बदल सकती है; इसलिए ऑब्जेक्ट और उसे प्राप्त करने की प्रक्रिया दोनों सुरक्षित रखें।

कैप्चर में पृष्ठ पहचानने के लिए पर्याप्त संदर्भ हो, लेकिन अनावश्यक डेटा उजागर न हो। उपयोगी और वैध होने पर HTML फ़ाइल, मल्टीमीडिया संसाधन और मूल प्रारूप में निर्यात साथ रखें तथा जो प्राप्त नहीं हो सका उसका विवरण दें। डाइनामिक पृष्ठ प्रत्येक आगंतुक को अलग सामग्री दिखा सकता है; रिपोर्ट उसे सार्वभौमिक दृश्य न माने।

4.2 प्रकाशन, थ्रेड और मल्टीमीडिया

पाठ, कथित लेखक, प्रकाशन पहचानकर्ता, दिखने वाली तिथि, URL, प्रासंगिक उत्तर, उद्धरण, रीपोस्ट, प्रतिक्रियाएँ और मल्टीमीडिया सुरक्षित रखें। एल्गोरिदम या मॉडरेशन से उत्तरों का क्रम बदल सकता है। थ्रेड कैप्चर करने पर दर्ज करें कि स्क्रॉल कैसे किया गया और कवरेज कहाँ तक थी। संदर्भ से बाहर एकल उत्तर वार्तालाप को विकृत कर सकता है।

अधिकृत होने पर छवि या वीडियो फ़ाइल डाउनलोड करें और उसका अलग हैश निकालें। मैनिफ़ेस्ट में प्रकाशन को फ़ाइल से संबद्ध करें। सामग्री की प्रामाणिकता जाँचनी हो तो मल्टीमीडिया विश्लेषण वाले विशिष्ट खंड का उपयोग करें; संरक्षण केवल यह सिद्ध करता है कि वह संस्करण उस स्रोत पर उस समय उपलब्ध था।

4.3 वेब संग्रह और तीसरे पक्ष की तिथियाँ

तीसरे पक्ष का वेब संग्रह उपयोगी स्नैपशॉट रख सकता है, लेकिन उसकी तिथि उसके कैप्चर की है, आवश्यक रूप से पहले प्रकाशन की नहीं। दर्ज करें कि किसने संग्रहित किया, कौन-सा संस्करण कैप्चर हुआ, कौन-से संसाधन नहीं मिले और उसे कैसे देखा गया। सामग्री में दी गई तिथि लेखक द्वारा संपादित हो सकती है या दूसरा समय क्षेत्र दिखा सकती है। पुष्टि के लिए समीपवर्ती तिथियों के प्रकाशन, सूचनाएँ, लिंक और रिकॉर्ड खोजें।

तत्व	आवश्यक रिकॉर्ड	सीमा
URL और रीडायरेक्ट	पूरा पता और पहुँच का क्रम।	बदलने वाला या वैयक्तिकृत सामग्री।
प्रकाशन और थ्रेड	पहचानकर्ता, पाठ, उत्तर और कैप्चर का गहरा कवरेज।	यदि कवरेज सीमित था, तो पूरा वार्तालाप नहीं।
मल्टीमीडिया	फ़ाइल, गुणवत्ता, हैश और उद्गम।	दृश्य की प्रामाणिकता या लेखकत्व सिद्ध नहीं।
बाहरी संग्रह	फ़ास्टडाकता, स्नैपशॉट, तिथि और अनुपस्थित संसाधन।	पहला प्रकाशन या पूर्ण सामग्री सिद्ध नहीं।
पहुँच	खाता, भूमिका, दृश्यता और प्रतिबंध।	ज़रूरी नहीं कि सभी उपयोगकर्ताओं ने एक जैसा देखा हो।

प्रस्तुत करने का नियम

वेब संग्रह के आधार पर “यह हमेशा ऐसा था” न कहें और कैप्चर के आधार पर “यही सब है” न कहें। उस संस्करण, तिथि और कवरेज का वर्णन करें जिसे वास्तव में सिद्ध किया जा सके।



चित्र 3. प्रकाशन का उसके परिवेश के साथ सुरक्षित रखा जाता है। कैप्चर एक प्रतिनिधित्व है, पूरा संसार नहीं। संपादकीय पुनर्निर्माण; वास्तविक प्रमाण नहीं।

अध्याय 5. दस्तावेज़ित संरक्षण और प्रमाणन

5.1 अधिग्रहण-अभिलेख

अधिग्रहण-अभिलेख में मामला, ऑपरेटर, अधिकार, स्थान, तिथि और समय क्षेत्र, डिवाइस, ब्राउज़र या उपकरण, खाता और भूमिका, प्राप्त ऑब्जेक्ट, कार्रवाइयाँ, प्रारूप, समस्याएँ और हैश दर्ज हों। स्क्रीन कैप्चर हो तो क्रम और फ़िल्टर बताएँ। निर्यात हो तो पैरामीटर और आउटपुट बताएँ। प्रदाता का उपयोग हो तो उसकी प्रतिक्रिया और चैनल सुरक्षित रखें। अभिलेख वास्तव में की गई कार्रवाई का वर्णन करता है, किसी ऐसी आदर्श प्रक्रिया का नहीं जो हुई ही नहीं।

संरक्षण प्रमाणपत्र अखंडता और सुलभता के प्रमाण का पूरक हो सकता है। मेक्सिको में NOM-151 अपने दायरे में डेटा संदेशों के संरक्षण और डिजिटलीकरण के लिए विशिष्ट आवश्यकताएँ रखती है; यह सामग्री की सत्यता प्रमाणित नहीं करती और पूरे संदेश के अधिग्रहण का विकल्प नहीं है। टाइमस्टैम्प या हैश मानव लेखकत्व या प्राप्ति की वैधता सिद्ध नहीं करता।[4][5]

5.2 कस्टडी और पहुँच नियंत्रण

स्रोत को कार्य-प्रति से अलग रखें और पहुँच सीमित करें। इलेक्ट्रॉनिक स्थानांतरण में प्राप्तकर्ता, अनुमतियाँ, तिथि, संस्करण, कुंजी डिलीवरी का चैनल और डाउनलोड सत्यापन शामिल हों। रिपोर्ट में पासवर्ड, टोकन या कुकीज़ न हों। प्रमाणीकृत पृष्ठ सुरक्षित करते समय सत्र उजागर किए बिना भूमिका दस्तावेज़ित करें।

कार्य-प्रति का उपयोग विश्लेषण, अनामीकरण और प्रस्तुति के लिए करें। सार्वजनिक संस्करण की समीक्षा करें ताकि व्यक्तिगत डेटा, अंतरंग छवियाँ, पते और असंबंधित तीसरे पक्ष शामिल न हों। गोपनीयकृत संस्करण बनाने पर सुरक्षित पूर्ण संस्करण नष्ट न करें; उसकी पहुँच और बाद का उपयोग सीमित रखें।

[4] NOM-151-SCFI-2016, डेटा संदेशों का संरक्षण और डिजिटलीकरण, 30-03-2017 को प्रकाशित। अभिलेख, अखंडता, सुलभता और इलेक्ट्रॉनिक डिजिटल फ़िंगरप्रिंट संबंधी आवश्यकताएँ। आधिकारिक ऑनलाइन स्रोत

[5] Secretaría de Economía. PLATIICA. NOM-151-SCFI-2016 का विवरण-पृष्ठ, डेटा संदेशों का संरक्षण और डिजिटलीकरण। वर्तमान वैधता की जाँच तथा DOF पाठ का पूरक संदर्भ। आधिकारिक ऑनलाइन स्रोत

5.3 विशेषज्ञ, नोटरी या प्रशासनिक प्रमाणन

चुनाव क्षेत्राधिकार, ऑब्जेक्ट और उद्देश्य पर निर्भर करता है। नोटरी कार्यवाही किसी दृश्य का दस्तावेज़ीकरण कर सकती है; विशेषज्ञ परीक्षण उद्गम, संरचना, प्रामाणिकता, संबंधों और संदर्भ का विश्लेषण कर सकता है; प्रशासनिक प्रमाणपत्र अपने दायरे की कार्रवाई सिद्ध कर सकता है। कोई भी किसी अंश को पूर्ण प्रमाण में नहीं बदलता। पृष्ठ बदल सकता है, इसलिए कार्रवाई दोहराने से बचने के लिए शुरू करने से पहले उपयुक्त प्रारूप का अनुरोध करें।

> **गुणवत्ता मानदंड**
> सबसे अच्छा प्रमाणन वह नहीं जिसमें सबसे अधिक मुहरें हों, बल्कि वह जिससे दूसरा व्यक्ति समझ सके कि क्या देखा गया, कहाँ, कब, किस विधि से और क्या बाहर रहा।

अध्याय 6. हटाना, शिकायत और मीडिया-क्षति

6.1 निकालने से पहले संरक्षित करें

सामग्री हटाने का अनुरोध करने से पहले URL, पहचानकर्ता, प्रकाशन, खाता, मल्टीमीडिया, उत्तर और पहुँच की तिथि सुरक्षित रखें। पहले से बदले हुए संस्करण और संदर्भ लिंक भी दर्ज करें। तात्कालिक खतरा हो तो सुरक्षा और आपातकालीन चैनलों को प्राथमिकता दें; संरक्षण खतरनाक देरी का कारण न बने।

प्लेटफ़ॉर्म को भेजी जाने वाली रिपोर्ट विशिष्ट हो: ऑब्जेक्ट, URL, कारण, प्रमाण, तिथि और अनुरोध। इसमें आवश्यकता से अधिक व्यक्तिगत डेटा न हो और हानिकारक फ़ाइल ऐसे चैनल पर न भेजी जाए जो इसके लिए निर्धारित नहीं है। रिपोर्ट संख्या, सामग्री, तिथि और उत्तर सुरक्षित रखें। लिंक हटने से यह सिद्ध नहीं होता कि सभी प्रतियाँ गायब हो गईं या क्षति समाप्त हो गई।

6.2 क्षति और पहुँच

विश्लेषण सामग्री, पुनःप्रकाशन, दिखने वाली पहुँच, प्रतिक्रियाएँ और बताए गए परिणामों को अलग करता है। प्लेटफ़ॉर्म काउंटर के अर्थ अलग हो सकते हैं; वे व्यक्तिगत पाठकों या कुल प्रभाव को सिद्ध नहीं करते। ज्ञात होने पर मेट्रिक्स को तिथि और अर्थ सहित सुरक्षित रखें। आधारहीन इम्प्रेशन को गुणा करके आर्थिक क्षति की गणना न करें।

मीडिया-क्षति के मूल्यांकन के लिए साक्ष्य, रोज़गार दस्तावेज़, अनुबंध, संचार और अन्य गैर-डिजिटल स्रोत आवश्यक हो सकते हैं। तकनीकी संरक्षण सामग्री और क्रम सिद्ध करता है, समस्त क्षति नहीं। रिपोर्ट गुमनाम खातों के धारक न बनाए और न किसी प्रकाशन के लहज़े से उनका उद्देश्य तय करे।

6.3 एकीकृत मामला

किसी काल्पनिक प्रकाशन में आरोप और कई उत्तर हैं। उपलब्ध थ्रेड, फ़ाइलें और मेट्रिक्स तिथि सहित सुरक्षित रखें। इसके बाद खाता पाठ बदलता है और एक उत्तर हटाता है। पहला संस्करण अपनी सीमाओं सहित और नया संस्करण संबंधित ऑब्जेक्ट के रूप में सुरक्षित रखें। विश्लेषण इतिहास मिटाए बिना बदलावों की तुलना करता है। हटाने का अनुरोध दर्ज करें, लेकिन रिपोर्ट यह न कहे कि सामग्री दूसरे खातों में फैलना बंद हो गई।

> **सबक**
> मीडिया-क्षति का प्रमाण संस्करणों और संदर्भ से बनता है। अंतिम कैप्चर पहले से कम दिखा सकता है, लेकिन पहला भी पूरे क्रम को सिद्ध नहीं करता।

परिशिष्ट A. संरक्षण प्रारूप

A.1 ईमेल-अभिलेख

काल्पनिक रिकॉर्ड

मामला / विषय: EXP-DEMO-2026-008 / EML-001-R00
स्रोत: [मेलबॉक्स, सर्वर, क्लाइंट या तीसरा पक्ष]
प्राप्ति: [निर्यात, डाउनलोड या डिलीवरी]
कथित प्रेषक और प्राप्तकर्ता: [रिकॉर्ड]
संदेश की तिथि और समय क्षेत्र: [यथावत]
अधिग्रहण की तिथि और समय क्षेत्र: [यथावत]
मुख्य भाग और विवरण: [संदर्भ, एल्गोरिदम और हैश]
हेडर: [पूरी फ़ाइल]
संलग्नक: [नाम, आकार, प्रारूप और हैश]
प्रमाणीकरण: [DKIM / SPF / DMARC, यदि जाँचा गया हो]
सत्यापन: [मेल और अंतर]
समस्याएँ: [प्रारूप, अनुपस्थिति, त्रुटि या सीमा]
कस्टडी: [मूल, कार्य-प्रति और पहुँच]

A.2 प्रकाशन रिकॉर्ड

फ़ील्ड	न्यूनतम सामग्री	निष्कर्ष
URL और पहचानकर्ता	पूरा पता, पैरामीटर और रीडायरेक्ट।	पता लगाने योग्य ऑब्जेक्ट।
खाता और कृत्य	कथित लेखक, सूचना, पहुँच और दिखने वाले दर्शक।	स्वचालित त्रुटि-आरोपण नहीं।
तारीखें	दिखने वाली तिथि, अवग्रहण, समय क्षेत्र और सटीकता।	प्रकाशन और डाउनलोड को एक न समझें।
सामग्री	पाठ, उत्तर, प्रतिक्रियाएँ, मल्टीमीडिया और संस्करण।	ब्रेक की कवरेज।
प्रक्रिया	उपकरण, संस्करण, फ़िल्टर और कार्यवाहियाँ।	पहरेदार की क्षमता।
फ़ाइल	HTML, छाप, पीडीएफ, निर्यात और हश।	मूल / व्युत्पन्न वस्तु की संपत्ति।
समस्याएँ	त्रुटि, पहुँच, अनुपस्थित सामग्री और सीमा।	कवरेज में छिपाएँ।

A.3 ऑब्जेक्ट मैनिफ़ेस्ट

डिलीवरी का सूचक

ID / मूल नाम / ऑब्जेक्ट का प्रकार
स्रोत और संबंध: [मूल, निर्यात, व्युत्पन्न]
प्राप्ति की तिथि और समय क्षेत्र
विधि और उपकरण / संस्करण
आकार और प्रारूप
ऑब्जेक्ट का एल्गोरिथ्म और हैश
पैरेंट ऑब्जेक्ट और संबंधित ऑब्जेक्ट
खोलना और सत्यापन
संवेदनशील डेटा और प्रतिबंध
संरक्षित स्थान और कार्य-प्रति
स्थानांतरण और प्राप्तकर्ता
सीमाएँ और लंबित कार्य

A.4 हटाने के अनुरोध का रिकॉर्ड

काल्पनिक प्रारूप

प्लेटफॉर्म और चैनल: [आधिकारिक]
URL / प्रकाशन / खाता: [विशिष्ट ऑब्जेक्ट]
कारण और संलग्न प्रमाण: [पहचानकर्ता]

अनुरोध: [हटाना, समाधान, संरक्षण]
तिथि और समय क्षेत्र: [भेजना]
रिपोर्ट संख्या: [संदर्भ]
उत्तरः [तिथि, सामग्री और कार्रवाई]
अन्य ज्ञात प्रतियां: [URL और स्थिति]
प्रभावित व्यक्तियों से संचार: [चैनल और संस्करण]
लंबित कार्य: [कवरेज और अगली समीक्षा]

परिशिष्ट B. कानूनी ढाँचा और अंतिम सूची

मेक्सिको CCom 89–94 और 1205 में डेटा संदेशों को मान्यता देता है; CFPC/CNPCF संक्रमणकालीन प्रावधानों के अनुसार विश्वसनीयता, प्रेषक से संबद्धता और अखंडता का विकास करता है; NOM-151 अपने दायरे में संरक्षण विनियमित करता है। पेरू हस्ताक्षर, प्रक्रिया और संग्रह को अलग-अलग व्यवस्थित करता है; चिली हस्ताक्षर और तिथि में अंतर करता है; अर्जेंटीना विश्वसनीयता का मूल्यांकन करता है; कोलंबिया और इक्वाडोर प्रारूप, उद्गम, गंतव्य और तिथियाँ सुरक्षित रखने की आवश्यकता रखते हैं; स्पेन eIDAS, LEC और ट्रस्ट सेवाओं को जोड़ता है। कोई भी नियम किसी संदेश को केवल इलेक्ट्रॉनिक होने के कारण सत्य नहीं बनाता।678910111213141516

संरक्षण पर गोपनीयता और तीसरे पक्षों के अधिकारों की सीमाएँ भी लागू होती हैं। भूमिकाएँ, पहुँच और प्रसार सीमित करें; कार्य और सार्वजनिक संस्करण अलग रखें; अंतरंग सामग्री, नाबालिगों का डेटा, रहस्य या क्रेडेंशियल प्रकाशित न करें। प्रमाण अधिकृत चैनल और मैनिफ़ेस्ट के साथ दें, फ़ाइलों के सार्वजनिक संग्रह के रूप में नहीं।171819

जांच जोड़	स्वीकृति का प्रश्न
जाँच सूची	क्या EML, URL, फ़ाइल और लॉग उपलब्ध हैं?
प्रक्रिया	क्या यह देखा गया कि किसने, किस भूमिका, फ़ोल्डर और तिथि के साथ इसे प्राप्त किया?
जरूरत	क्या प्रत्येक हश किसी जाँच सूची से संबंधित है?

[6]मेक्सिको की वाणिज्य संहिता, अनुच्छेद 89–94 और 1205: तटस्थता, प्रेषक से संबद्धता, लिखित रूप, मूल, अखंडता, सुलभता और डेटा संदेशों की स्वीकार्यता। आधिकारिक संकलन। आधिकारिक ऑनलाइन स्रोत

[7]राष्ट्रीय नागरिक और पारिवारिक प्रक्रिया संहिता, अनुच्छेद 348–350। 15-01-2026 के संशोधन सहित संकलन। इसका लागू होना क्रमिक है और आधिकारिक घोषणाओं पर निर्भर करता है। आधिकारिक ऑनलाइन स्रोत

[8]NOM-151-SCFI-2016, डेटा संदेशों का संरक्षण और डिजिटलीकरण, 30-03-2017 को प्रकाशित। अभिलेख, अखंडता, सुलभता और इलेक्ट्रॉनिक डिजिटल फ़िंगरप्रिंट संबंधी आवश्यकताएँ। आधिकारिक ऑनलाइन स्रोत

[9]पेरू. IOFE विनियमन, DS 052-2008-PCM, अनुच्छेद 3 और 4: डिजिटल रूप से हस्ताक्षरित इलेक्ट्रॉनिक दस्तावेजों की आवश्यकता और स्वीकृति। आधिकारिक ऑनलाइन स्रोत

[10]पेरू. सिविल प्रक्रिया संहिता, अनुच्छेद 188–197 और 245.5: उद्देश्य, वैधता, साधन, प्रमाण का भार, मूल्यांकन और तकनीकी साधनों से तिथि का निर्धारण। आधिकारिक ऑनलाइन स्रोत

[11]चिली. इलेक्ट्रॉनिक दस्तावेज़ों और इलेक्ट्रॉनिक हस्ताक्षर संबंधी कानून 19.799, अनुच्छेद 1–5: समकक्षता, लिखित रूप, साधारण/उन्नत हस्ताक्षर, तिथि और प्रमाणीय मूल्य। आधिकारिक ऑनलाइन स्रोत

[12]अर्जेंटीना. सिविल और वाणिज्यिक संहिता, अनुच्छेद 318–319: किसी भी माध्यम से पत्राचार तथा तकनीकी माध्यमों और प्रक्रियाओं की विश्वसनीयता का मूल्यांकन। आधिकारिक ऑनलाइन स्रोत

[13]कोलंबिया. 1999 का कानून 527, अनुच्छेद 5–13, 16–25 और 28: डेटा संदेश, लिखित रूप, मूल, अखंडता, स्वीकार्यता, संरक्षण, भेजना, प्राप्ति और डिजिटल हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[14]इक्वाडोर. इलेक्ट्रॉनिक वाणिज्य, इलेक्ट्रॉनिक हस्ताक्षर और डेटा संदेश कानून, कानून 67, अनुच्छेद 2, 6–8, 10–16: समकक्षता, लिखित रूप, मूल, संरक्षण, उद्गम, भेजना, प्राप्ति और इलेक्ट्रॉनिक हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[15]विनियमन (UE) 910/2014 eIDAS, अनुच्छेद 25–26 और 46: प्रारूप के कारण इलेक्ट्रॉनिक हस्ताक्षरों और दस्तावेज़ों से भेदभाव न करना, उन्नत हस्ताक्षर और क्वालिफ़ाइड हस्ताक्षर के प्रभाव। आधिकारिक ऑनलाइन स्रोत

[16]स्पेन. सिविल प्रक्रिया कानून, अनुच्छेद 326 और 384: निजी दस्तावेज़, चुनौती, डेटा को संग्रहित, जानने या पुनः उत्पन्न करने के साधन, परीक्षा, कस्टडी और सुदृढ़ न्यायिक मूल्यांकन। आधिकारिक ऑनलाइन स्रोत

[17]मेक्सिको. निजी क्षेत्र के व्यक्तियों के पास मौजूद व्यक्तिगत डेटा के संरक्षण संबंधी संघीय कानून, 20-03-2025 को प्रकाशित पाठ और 14-11-2025 का संशोधन। अनुच्छेद 5–9, 18–20 और 31: सिद्धांत, सुरक्षा, गोपनीयता, उल्लंघन और अधिकारों का निपटान। वर्तमान संघीय प्राधिकरण Secretaría Anticorrupción y Buen Gobierno है। आधिकारिक ऑनलाइन स्रोत

[18]कोलंबिया. 2012 का विधान कानून 1581, अनुच्छेद 4, 8, 12, 17–18 और 26: सिद्धांत, अधिकार, सूचना, नियंत्रकों और प्रोसेसरों के कर्तव्य तथा तीसरे देशों में स्थानांतरण। आधिकारिक ऑनलाइन स्रोत

[19]यूरोपीय संघ. विनियमन (UE) 2016/679, अनुच्छेद 5, 25, 28 और 32–34: सिद्धांत, डिज़ाइन से सुरक्षा, प्रोसेसर, सुरक्षा और सुरक्षा उल्लंघनों की अधिसूचना/संचार। स्पेन में लागू राष्ट्रीय और क्षेत्रगत कानून की भी समीक्षा आवश्यक है। आधिकारिक ऑनलाइन स्रोत

जाँच का क्षेत्र	स्वीकृति का प्रश्न
पेनल	क्या DKIM / SPF / DMARC की व्याख्या उनकी सामाजिक सहमति की गई?
कवरेज	क्या ब्रेड, उत्तर और अनुपस्थितियाँ स्पष्ट रूप से दर्ज हैं?
अट्रिब्यूशन	क्या खोत और व्यक्ति के बीच भ्रम नहीं रखा गया?
गोपनीयता	क्या डिलीवरी में जनोपरक्षक उल्लंघन होने से बचा गया है?

समापन

संरक्षण का अर्थ किसी समय मौजूद चीज़ का सत्यापनयोग्य मार्ग छोड़ना है। जब तक पर्याप्त न लगे, तब तक स्क्रीनशॉट इकट्ठा करते रहना नहीं।