

ISEC7
THE DIGITAL WORKPLACE COMPANY

ISEC7 CLASSIFY

No classification, no sending.

Users classify confidential documents correctly and share them only with the right people, in every Office application and on every device. ISEC7 CLASSIFY checks the recipients before a message is sent.

One interface
Microsoft Outlook on desktop and on the web, Android, iOS

NATO, TLP, USCLASS
ready-made profiles, US schemes on authorized request

Works with Purview
labels synchronized in both directions

Data sovereignty
sovereign software from Germany by the ISEC7 Group

CHALLENGE

Without classification, cybersecurity is flying blind.

Firewall, EDR and SOC are in place. But do you know which data is critical, who receives it and what must never get out? ISO/IEC 27001:2022 has two controls for exactly that: A.5.12 for classifying and A.5.13 for labeling information. Anyone working for US government customers needs verified, enforced data markings under DoD Manual 5200.01, DoD Instruction 5200.48 (CUI) and CMMC.

CAPABILITIES

Users classify emails, attachments and Office documents in the applications they already work in. Before a message is sent, ISEC7 CLASSIFY checks its classification against the recipient addresses.

- Mandatory fields: incomplete markings block sending and saving, including calendar entries and documents where supported
- Domain check: confidential content addressed to foreign domains is blocked or flagged
- Every attachment is marked individually
- Every section individually: subject, text or paragraphs, with banners, caveats and handling instructions
- Network-aware: available classification levels follow the security level of the network

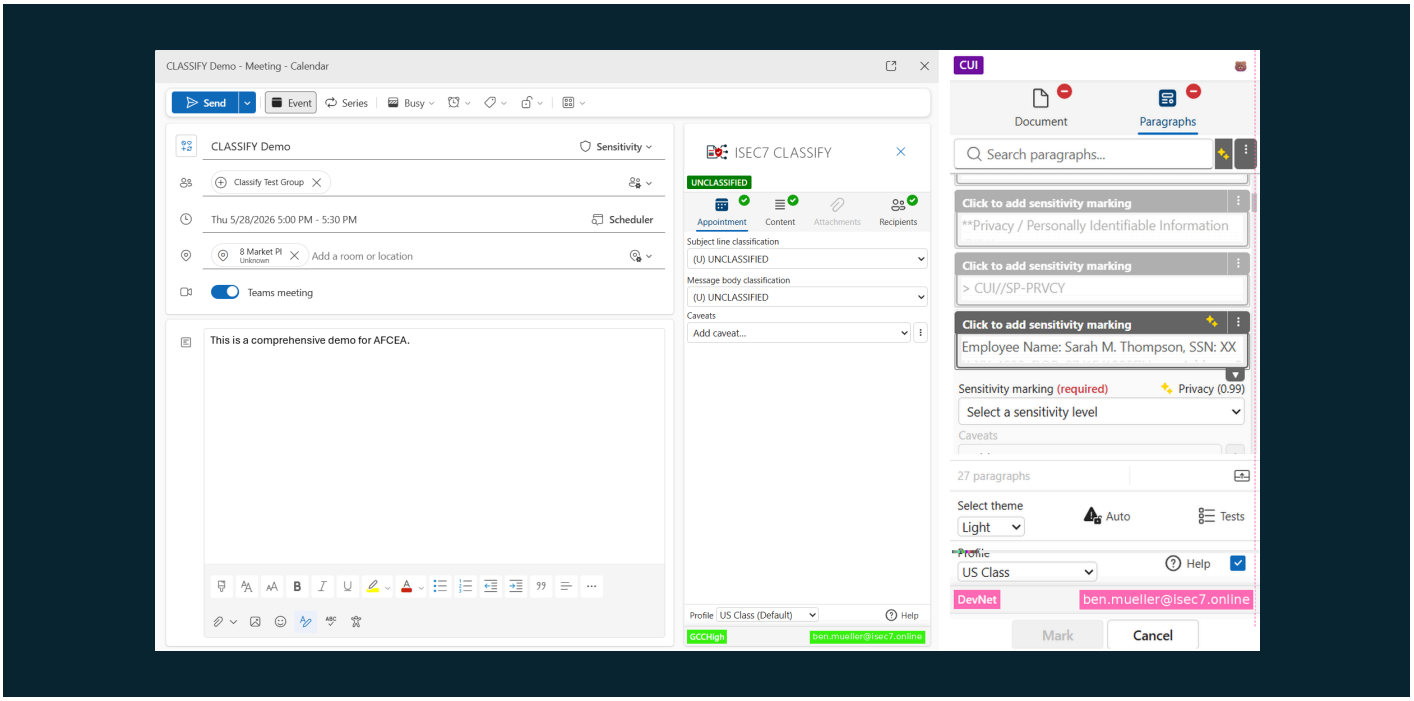
THE SOLUTION & USP

- One interface on all clients: Microsoft Outlook, Outlook on the web, Word, Excel, PowerPoint and SharePoint, plus ISEC7 MAIL on iOS and Android, for Microsoft 365 and on-premises environments
- Multiple schemes at the same time: users switch between profiles
- Multilateral: classification across organizational boundaries, between countries, units, AD groups and individual users
- Ready-made standards and your own schemes: BUND, NATO and TLP are included. US schemes (USCLASS, CUI) are available on authorized request. You build your own schemes in the ISEC7 SPHERE Schema Editor
- Hosted on Microsoft Azure as Platform as a Service (PaaS), no desktop installation required
- Continuous audit: audit trails and statistics in ISEC7 SPHERE, including SharePoint and Teams

TARGET GROUP

- Government agencies and organizations with security requirements (NIS2, BOS, KRITIS)
- Public sector organizations working under the VSA or an ISMS
- Companies that share sensitive information along the supply chain
- Companies with confidential know-how or intellectual property to protect

Since 2003, the ISEC7 Group has run Digital Workplace and Managed Mobility Services for public authorities, international enterprises, operators of critical infrastructure (KRITIS), companies that handle classified information and other organizations with strict compliance requirements. Over 700 customers worldwide, among them governments, police forces and armed forces. ISEC7 is headquartered in Germany, with locations in the USA, Australia, New Zealand and Poland.



ISEC7 CLASSIFY AND MICROSOFT PURVIEW

CLASSIFY once, protected everywhere.

Sensitivity labels in Microsoft Purview trigger encryption, marking and access rules. ISEC7 CLASSIFY offers native Microsoft Information Protection (MIP) integration, with labels synchronized in both directions. And it goes further: it runs on PCs, in Microsoft 365 and on mobile devices, and checks before sending whether the recipients are authorized for the classification.

AREAS OF APPLICATION

- Word, Excel, PowerPoint: marking down to individual paragraphs and cells, every slide shows its level
- SharePoint Online: three banner levels (tenant, site, page), marking down to folder and file names

LOCAL AI

The AI runs locally only, with no internet connection. No data leaves the device.

- Recognizes sensitive content and alerts the user until a marking is selected
- Suggests a marking for each section; a sensitivity score indicates relevance
- Models: CUI/NIS2 (English, German) with 115 CUI subcategories for sensitivity markings, Security Classification Guide (English) for classification

US REQUIREMENTS

- CUI under 32 CFR 2002 and DoD Instruction 5200.48, with a prefilled CUI designation indicator and authority block
- DoD Manual 5200.01: banner, portion and subject line marking, with caveat controls
- CMMC 2.0 and NIST SP 800-171: audit trails in ISEC7 SPHERE provide evidence for assessment readiness. ISEC7 is not a C3PAO
- DFARS 252.204-7019: supports DoD contractors handling CUI, with NIST SP 800-171 alignment
- DoD Zero Trust: classification and tagging in the data pillar (Activity 3.2.2), plus FISMA
- CSfC: with ISEC7 SPHERE, meets the Mobile Access Capability Package and continuous monitoring requirements
- NIPRNet, SIPRNet and JWICS. Microsoft 365 GCC, GCC High and DoD, FedRAMP Authorized Path

FIND OUT MORE

www.isec7.com/en/solutions/isec7-classify