Microsoft 365 Security Best Practices Licensing Matrix

LEGEND

- BP = Microsoft 365 Business Premium
- E1 = Microsoft 365 Enterprise E1
- E3 = Microsoft 365 Enterprise E3
- E5 = Microsoft 365 Enterprise E5 (or E3 + equivalent security add-ons)
- A1 / A3 / A5 = Education versions of E1 / E3 / E5 (similar feature tiers, tailored for schools and universities)
- Sec Add-on = Microsoft 365 E5 Security add-on or equivalent standalone SKU (e.g., Defender for Endpoint P2, Entra ID P2, Purview Compliance add-on)

1. Identity & Access Management (IAM)

Best Practice	BP	E1	E3	E5	Sec Add-on
MFA for all users	✔	✔	✔	✔	
Phishing-resistant MFA (FIDO2, number matching)	✔	✔	✔	✔	
Block legacy authentication	✔	✔	✔	✔	
Conditional Access policies	✔	✘	✔	✔	
Risk-based sign-in policies	✘	✘	✘	✔	(Entra ID P2)
Just-in-Time (JIT) admin access via PIM	✘	✘	✘	✔	(Entra ID P2)
Just-Enough-Access (JEA)	✘	✘	✘	✔	(Entra ID P2)
Remove standing global admins	✔	✔	✔	✔	
Cloud-only admin accounts with MFA/PIM	✔	✔	✔	✔	(PIM requires E5/P2)
Monitor admin role assignments	✘	✘	✘	✔	(Entra ID P2)
Certificate-Based Authentication	✘	✘	✔	✔	
External collaboration access controls	✔	✔	✔	✔	
Guest access expiry & reviews	✘	✘	✘	✔	(Entra ID P2)
Illicit app consent detection	✘	✘	✘	✔	(MCAS/E5 Sec)
RBAC least privilege	✔	✔	✔	✔	

2. Advanced Threat Protection (ATP)

Best Practice	BP	E1	E3	E5	Sec Add-on
Safe Attachments (email, SPO, ODB, Teams)	✔	✘	✘	✔	(Defender for O365 P1/P2)
Safe Links	✔	✘	✘	✔	(Defender for O365 P1/P2)
Anti-phishing (impersonation, spoof)	✔	✘	✘	✔	(Defender for O365)
Domain impersonation protection	✔	✘	✘	✔	
Block high-risk file types	✔	✔	✔	✔	
Block macros from internet	✔	✔	✔	✔	
Zero-Hour Auto Purge (ZAP)	✔	✘	✘	✔	
SPF/DKIM/DMARC enforcement	✔	✔	✔	✔	
Threat Explorer	✘	✘	✘	✔	(Defender for O365 P2)
Defender for Endpoint (EDR)	✔ (P1)	✘	✘	✔	(P2)
Defender for Identity	✘	✘	✘	✔	
Suspicious email pattern alerts	✔	✘	✘	✔	
Block auto-forward to external	✔	✔	✔	✔	
Microsoft Sentinel integration	✘	✘	✘	✔	(Standalone Sentinel)

3. Information Protection & Data Governance

Best Practice	BP	E1	E3	E5	Sec Add-on
Data classification taxonomy	✔	✔	✔	✔	
Sensitivity labels with encryption & marking	✔	✘	✔	✔	
Auto-labeling	✘	✘	✘	✔	(Purview Auto-Labeling)
DLP (email, SPO, ODB, Teams)	✔	✘	✔	✔	
DLP integrated with sensitivity labels	✔	✘	✔	✔	
Retention labels/policies	✔	✘	✔	✔	
Records management	✘	✘	✘	✔	(Purview Records Mgmt)
Encryption at rest & transit	✔	✔	✔	✔	
Purview Scanner for on-prem data	✘	✘	✘	✔	
Extended audit log retention	✘	✘	✘	✔	
Insider risk management	✘	✘	✘	✔	
Default link type = “Specific people”	✔	✔	✔	✔	
Block download to unmanaged devices	✔	✘	✔	✔	
File block settings in Office apps	✔	✔	✔	✔	
Content marking	✔	✘	✔	✔	
Suspicious file activity alerts	✔	✘	✔	✔	

4. Device Management

Best Practice	BP	E1	E3	E5	Sec Add-on
Device enrollment required	✔	✘	✔	✔	
Device compliance policies	✔	✘	✔	✔	
Full disk encryption	✔	✘	✔	✔	
Device integrity checks	✔	✘	✔	✔	
Conditional Access requires compliance	✔	✘	✔	✔	
App protection for BYOD	✔	✘	✔	✔	
Defender for Endpoint	✔ (P1)	✘	✘	✔	(P2)
Attack Surface Reduction rules	✔	✘	✔	✔	
Device risk-based access control	✘	✘	✘	✔	(Defender for Endpoint P2 + CA)
OS & patch compliance	✔	✘	✔	✔	
Mobile Threat Defense integration	✔	✘	✔	✔	
Block unsupported/jailbroken devices	✔	✘	✔	✔	
Device risk scoring/alerts	✘	✘	✘	✔	
Cloud admin access limited to managed devices	✔	✘	✔	✔	
Stale device removal	✔	✔	✔	✔	

5. Application & Collaboration Hardening

Best Practice	BP	E1	E3	E5	Sec Add-on
External sharing limits	✔	✔	✔	✔	
Guest access controls	✔	✔	✔	✔	
Tenant creation/app registration restricted	✔	✔	✔	✔	
Admin approval for app consent	✔	✔	✔	✔	
Client app policies for mobile	✔	✘	✔	✔	
Legacy add-ins & macros blocked	✔	✔	✔	✔	
Safe Links/Safe Attachments in collaboration tools	✔	✘	✘	✔	
Sensitivity labels on shared files	✔	✘	✔	✔	
Teams security & governance	✔	✔	✔	✔	
Office apps hardened	✔	✔	✔	✔	
OLE package restrictions	✔	✔	✔	✔	
Suspicious file sharing alerts	✔	✘	✔	✔	
Public Teams/Site creation restricted	✔	✔	✔	✔	
Default link types/expiration	✔	✔	✔	✔	
Block downloads to unmanaged devices	✔	✘	✔	✔	
File type blocking in SPO/ODB	✔	✔	✔	✔	

6. Monitoring & Response

Best Practice	BP	E1	E3	E5	Sec Add-on
Unified Audit Log enabled	✔	✔	✔	✔	
Extended log retention	✘	✘	✘	✔	
Admin activity alerts	✔	✔	✔	✔	
High-risk user activity alerts	✔	✘	✔	✔	
Suspicious sign-in alerts	✔	✘	✔	✔	
Suspicious email alerts	✔	✘	✔	✔	
File activity monitoring	✔	✘	✔	✔	
Automated Incident Response (AIR)	✘	✘	✘	✔	
Microsoft Sentinel integration	✘	✘	✘	✔	(Standalone Sentinel)
MCAS alerts	✘	✘	✘	✔	
Entra ID Protection risk detection	✘	✘	✘	✔	
Threat hunting	✘	✘	✘	✔	
Incident response playbooks	✔	✔	✔	✔	
CoreView advanced alerting	✘	✘	✘	✔	(CoreView license)

7. System Security Management & Operations

Best Practice	BP	E1	E3	E5	Sec Add-on
Secure Score review	✔	✔	✔	✔	
Framework control mapping	✔	✔	✔	✔	
Security baselines enforced	✔	✘	✔	✔	
Change control	✔	✔	✔	✔	
Patch management	✔	✘	✔	✔	
Security audits & access reviews	✔	✔	✔	✔	
M365 backups tested	✔	✔	✔	✔	(Third-party required)
Phishing simulations	✔	✘	✔	✔	
Conditional Access review	✔	✘	✔	✔	
Exceptions register	✔	✔	✔	✔	
Automated executive reports	✔	✔	✔	✔	
Admin training	✔	✔	✔	✔	
Zero Trust gap analysis	✔	✔	✔	✔	
CoreView advanced alerting	✔	✔	✔	✔	

This table makes it instantly clear:

- **Microsoft 365 Business Premium** provides a strong baseline for SMBs, including Defender for Office 365 P1 and Defender for Endpoint P1.
- **Microsoft 365 Enterprise E3** delivers enterprise-grade compliance but lacks advanced identity risk detection and automated incident response.
- **Microsoft 365 Enterprise E5** (or Microsoft 365 E5 Security add-on) unlocks **P2 capabilities** such as Entra ID P2, Privileged Identity Management, Microsoft Defender for Office 365 P2, Microsoft Defender for Endpoint P2, advanced auditing, and Insider Risk Management.