Aragon Research

ENTERPRISE SECURITY CHECKLIST

Enterprise security is becoming increasingly important as cyber threats are growing. Enterprises need to put reliable and effective security measures in place to protect confidential data and information.

The following checklist provides you with aspects of security you must plan for in order to have a safe, well-functioning, and protected enterprise. While this checklist is not a replacement for a comprehensive strategy, you should use it to help identify what may be missing from your enterprise security plan.

AUDITS

Have you had an internal or external privacy audit in the past 12 months?	□
Have you had a security and compliance audit in the past 12 months?	□
If yes to above two sections, have all recommendations been implemented?	□
Have you undergone any information security compliance evaluations?	□
If yes, were you found to be in compliance?	□
Do you hire professionals to conduct audits to ensure compliance with your security policies?	□

CONTENT MANAGEMENT & DATA STORAGE

Is your content encrypted at rest?	□
Is your content encrypted in transit?	□
Do you store PII, PHI, or other confidential information on laptops, smartphones, memory sticks, or other mobile devices? If yes, is this information encrypted?	□
For your content that includes PII, do you have a GDPR compliant policy in place relative to PII?	□
Do you honor the privacy of customer data and get permission before sharing it with third parties?	□
Do you discard of data once it is no longer needed?	□
Do you have an effective method of discarding data once it is no longer needed?	□

PII: Personally Identifiable Information

PHI: Protected Health Information

GDPR: General Data Protection Regulation

Enterprises have to maintain critical content due to business and compliance regulations, and that has become the primary task for traditional ECM systems.

CYBERATTACKS & SECURITY BREACHES

Are your employees aware of the risks surrounding security breaches?	□
Does your enterprise have a written plan of action in the case of a cyberattack or security breach?	□
Do you practice cyber and natural disaster recovery drills?	□
Are your applications and devices disconnected when not in use?	□
Have you deployed Network Threat Protection? If yes, is your Network Threat Protection automatically updated by your vendor?	□
Have you deployed virus barrier and malware detection applications to employee computers?	□
Are your anti-malware programs set to automatically update?	□
Are your employees trained to connect securely to a VPN and avoid public networks?	□
Do you have a secure method for backup storage?	□
Do you regularly back up your enterprise data and devices?	□
Do your employees regularly backup their machines to the cloud or to a hard drive?	□
Do you have a data recovery and re-use solution in place?	□
Do you have enterprise backup software deployed for both devices and applications?	□
After a computer attack or loss of data, are you able to restore your operations within 24 hours?	□

DIGITAL TRANSACTION MANAGEMENT/ E-SIGNATURE

Do you use e-Signatures to verify identity during digital transactions?	□
Does your e-Signature of DTM provider meet security standards for identity, cloud and content storage, and replication?	□

MULTI- FACTOR AUTHENTICATION

Have you implemented multi-factor authentication across your enterprise applications?	□
Do your application providers enable you to mandate/enforce multi factor authentication among your employees and your executives?	□
Do you use an Identity and Access Management provider to manage multi-factor?	□

Two-Factor Authentication (2FA) is a type of multi-factor authentication that serves as an added layer of security to ensure that only verified personnel have access to accounts and information. It does this by confirming the user’s identity using the combination of two factors instead of giving access immediately.

EMAIL & CALENDAR

Do you have multi-factor authentication turned on for Email and Calendar?	□
Does your provider encrypt your email messages?	□
Do you use a firewall?	□
Does your enterprise implement a strong password policy for employees?	□
Does your email provider automatically flag suspicious emails?	□
Are members of your enterprise required to report suspicious emails and instructed to avoid opening them?	□

CALLS & MEETINGS

Are your employees aware of the risks associated with audio and video meeting tools?	□
Have you done a security audit of your web and video conferencing provider?	□
Have you done a security audit of your voice provider (i.e. on-premise or cloud PBX)?	□
Are your audio and video meetings encrypted?	□
Do you verify the security your UCC provider offers before assuming your meetings are protected?	□
Have you conducted a security audit of all UCC providers your employees use on their own?	□

UCC: Unified Communications and Collaborations

Audio and video calls and meetings present the risk of your conversations being recorded and your data being used without permission.

MONITORING

Do you regularly monitor user activity to watch for suspicious activity?	□
Do you closely monitor internal network traffic?	□
Do you practice equipment tracking?	□

PROVIDERS

Do your application providers meet privacy and security standards that are common best practices in their industry?	□
Is security a major factor you consider when evaluating a new technology solution?	□
Do you have a security checklist for new software and services providers?	□

PRIVACY POLICY & TERMS OF USE

Do you have your privacy policy listed on your website?	□
Do you have your terms of use listed on your website?	□

CONTRACTS & INTELLECTUAL PROPERTY

Are all of your customer contracts and agreements in written form?	□
Do you have a written program for managing intellectual property rights?	□
Do you develop contracts with those you hire to ensure ownership of intellectual property rights of the work they perform for your enterprise?	□
Do you handle customer complaints formally and document them in writing?	□
Do you obtain legal opinion on contracts?	□
Do you utilize a standard sub-contractor contract?	□

Having contracts and important agreements in writing is necessary to protect your enterprise in case of disagreements and misunderstandings within the organization or with outside parties.

HUMAN RESOURCES (HR)

Does HR conduct background checks for potential employees, leased workers, and contractors?	□
Do new employees undergo a security training program during onboarding?	□
Do you continue to train your employees on security best practices?	□
Does your employee exit procedure take security—both cyber and physical—into account?	□
Do you have a security protocol program for remote workers?	□
Do you have a designated person in charge of data/network security in your enterprise?	□

After finishing your checklist, we recommend immediate review of all unchecked boxes, as these will reveal the gaps in your security strategy.

Aragon Research can help you plan and execute security strategies specific to your enterprise.

Visit https://aragonresearch.com/contact/ to get started.