FAIR
Finnish AI Region | EDIH

Co-funded by the European Union

SMALL CYBER-SECURITY GUIDE

FOR SMEs

2/2025

everything you need is within your reach

Sinua varten

FAIR
Finnish AI Region | EDIH

Text: Martti Asikainen, Solja Sulkunen,
Jussi Rantsi ja Jenni Selosmaa
Edit and Layout: Martti Asikainen
Photos: Adobe Stock Photos
https://www.fairedih.fi

contents

INTRODUCTION

TThis guide is specifically designed for small and medium-sized enterprises (SMEs) and organisations with limited IT expertise who wish to implement artificial intelligence in their business operations safely and responsibly. The adoption of AI offers significant opportunities for streamlining processes, enhancing customer experience, and strengthening competitive advantage.

However, it also introduces new types of risks, particularly concerning data security and privacy protection. In this context, we define cybersecurity as all measures and practices aimed at protecting an organisation's data, systems, and operations from unauthorised access, misuse, disruption, or destruction. For AI solutions, this encompasses protecting models and data, authenticating users, and ensuring transparency and traceability of operations through various mechanisms and procedures.

Since AI solutions are often integrated with extensive information systems and therefore utilise vast amounts of data, their secure implementation requires a comprehensive approach. This involves not merely technical solutions, but also management commitment, staff training, and the establishment of clear policies and guidelines for every member of the organisation.

The purpose of our concise cybersecurity guide is to provide you with a clear and practical approach to the secure implementation of AI, as well as the development of information and cybersecurity capabilities within your organisation. Should any of the terms we use be unfamiliar to you, we have included a brief glossary at the end of this guide to facilitate your understanding of the text.

AN OVERVIEW OF IMMEDIATE MEASURES

The secure deployment of artificial intelligence requires combining multiple, mutually reinforcing cybersecurity measures. Careful validation and sanitisation of inputs prevents execution of malicious commands, while robust access control, encryption, and data classification protect critical system components and sensitive data. Defences against injection attacks, proactive threat monitoring, and regular testing, such as penetration tests and vulnerability assessments, enhance system resilience. Training and rehearsing with all staff, alongside clear action plans for incident scenarios, strengthen the organisation's ability to react swiftly and effectively to threats. AI itself can serve both as a shield and a vulnerability. Thus, safe usage demands integrating security throughout the development lifecycle from the outset. This chapter briefly outlines steps you can take immediately.

1. **Implementing strong access control mechanisms** is essential to cybersecurity in AI projects. Effective rights management is based on the principle of least privilege: users and systems should only be granted permissions necessary for their roles. **Access to AI systems should be restricted strictly to those who genuinely require it**. Privileges must be precisely defined for both data access and functional capabilities. It is advisable to implement multi-factor authentication for critical systems, as this adds a significant additional layer of security. Regular review and updating of user credentials is also crucial—former users pose as much risk as current ones.

2. **Protecting sensitive information across its entire lifecycle** is an integral part of AI project security. Utilising strong encryption for both storage and transmission of data is of paramount importance. **Encryption protocols** should be regularly updated to comply with the latest security standards, as cryptographic methods evolve continuously. It is also vital to identify and classify your company's data by sensitivity in order to apply appropriate protection measures to different data categories. Since AI systems often handle large volumes of data, proper information safeguarding becomes even more critical.

3. **AI systems can be particularly vulnerable to various injection attacks**, where malicious code is introduced into the system. **SQL injections** are common database attacks where adversaries manipulate queries to gain unauthorised access to data. **Command injections** attempt to coerce the system into executing malicious commands. In **cross-site scripting** (XSS), attackers inject malicious script code into web applications that is then executed in other users' browsers. To defend against these threats, it is essential to adhere to secure coding practices and ensure all inputs are meticulously validated and sanitised.

4. I**mplementing intrusion detection and prevention systems** is a key aspect of proactive security. These systems **actively monitor network traffic** to identify unusual activities that may signal security threats. Automated alerts for suspicious behaviour enable swift response to **potential risks**. Continuous, **real-time monitoring** is vital as cyber threats evolve constantly. AI-based threat detection systems can learn normal network behaviours and spot anomalies—even novel threats previously unseen.

5. **Regular security testing is crucial for identifying system vulnerabilities** before adversaries exploit them. Penetration testing simulates attack scenarios, helping discover and remediate security gaps. Vulnerability assessments offer a **systematic approach to identifying weaknesses** in systems and applications. Code reviews ensure that AI systems adhere to best security practices and standards. These tests should be performed regularly, as new vulnerabilities emerge over time and systems evolve through updates.

PREPARING FOR INCIDENT RESPONSE

Clearly documented guidelines for different cyber-threat scenarios are a fundamental component of a robust cybersecurity strategy. Organisations must prepare for denial-of-service (DoS/DDoS) attacks, data breaches, malware infections, and ransomware — any of which can compromise system availability or lead to the loss or misuse of sensitive information. Swift and effective response depends on having accessible and well-known procedures. Exercises and simulated disruption scenarios help employees understand roles and responsibilities during a crisis.

It is important to remember that **people are often the weakest link in cybersecurity**. Regular staff training is therefore essential to reduce risk and increase awareness. Simulated phishing campaigns, clear operational protocols, and AI-related security training help foster an organisational culture where cybersecurity is taken seriously and everyone understands their responsibilities.

Cybersecurity is not a single project that you tick off. It is a continuous process requiring ongoing attention, expertise, and development. As technology and threat landscapes evolve, checklists, protocols, and protective measures must be consistently updated. Adhering to secure coding practices, leveraging sector-specific security frameworks, and employing specialised security software enhance system defence and detect vulnerabilities before they can be exploited.

AI holds a dual role in cybersecurity. It can bolster protection but may also introduce new attack vectors. AI-powered solutions can analyse vast amounts of data, detect anomalies, and automate security tasks — but attackers can also harness AI for sophisticated scams and automated vulnerability scanning. Addressing these threats requires up-to-date expertise and continual vigilance.

Security planning should begin from the earliest stages of AI system development. By embedding security into the system architecture from the start — known as "security by design" — you avoid later remediation efforts that are often inefficient and costly. This proactive approach allows seamless integration of security into the system's operation.

For small and medium-sized enterprises, safe AI adoption requires a comprehensive cybersecurity strategy. Protecting inputs, managing access rights, encrypting data, and preventing injection attacks lay the foundation for a secure AI solution. Alongside these, develop mechanisms for threat detection, regular testing, and continuous preparation for various disruption scenarios. It's equally important to acknowledge the human factor and ensure staff engagement in a security-aware culture. Cybersecurity is not a destination, but a continual process of adaptation and learning.

AI can be a powerful tool in enhancing security—but it can also open new attack pathways. That is why ongoing evaluation, training, and proactive measures are indispensable.

At the end of this brief guide you will find links to useful materials, trainings, and services that support your organisation on the journey. Remember, cybersecurity is not a destination — it is a process of continual adaptation and learning.

Cybersecurity in Practice

Continuous process. Cybersecurity requires continuous monitoring, testing and updating of protective measures.

AI's dual role. Artificial intelligence can improve cybersecurity, but it can also be exploited for sophisticated attacks.

Security planning from the outset. The security by design principle means that protection is built into the system architecture during the development phase.

Comprehensive approach. Safe AI deployment requires consideration of technical, organisational and human factors.

DIFFERENCE BETWEEN CYBERSECURITY AND INFORMATION SECURITY?

Information security and cybersecurity, though often used interchangeably in professional discourse, represent distinct approaches to safeguarding an organisation's valuable assets. While the two fields share considerable overlap, a nuanced understanding of their differences is essential for organisations aiming to develop robust security frameworks. Information security refers to the protection of information assets, regardless of their form—whether digital, physical, or intellectual. It is underpinned by the foundational principles of the CIA triad: confidentiality, integrity, and availability. The scope of information security encompasses all formats of information, including physical documents, verbal communication, and institutional knowledge retained by personnel.

Cybersecurity, by contrast, focuses specifically on protecting digital assets from threats originating in the cyber domain. Its core objective is to defend systems, networks, and digital infrastructure against malicious activities within virtual environments. While information security has been a concern since organisations first recognised the need to safeguard sensitive data, cybersecurity has emerged in tandem with the growth of computer networks and digital technologies.

> **“Cybersecurity focuses specifically on protecting digital assets from threats originating in the cyber domain.”**

The primary distinction lies in their respective scopes: information security implements comprehensive policies to protect all forms of information, whereas cybersecurity concentrates on technological defences against digital threats. For example, information security measures may include physical safeguards such as secure document disposal and workplace access controls, while cybersecurity involves technical mechanisms like firewalls, intrusion detection systems, and vulnerability management frameworks.

This distinction is critical because a resilient security architecture requires the integration of both approaches. Organisations that focus solely on cybersecurity may overlook physical vulnerabilities or insider threats, while those relying exclusively on traditional information security practices may be inadequately prepared to counter sophisticated cyber attacks. It is also worth noting that cyber threats encompass more than technical exploits—they include a wide range of malicious influence operations. While cybercrime is often financially motivated, it can also be driven by political agendas or simply by the thrill of the challenge. As organisational environments become increasingly digitised, the boundary between these disciplines continues to blur. The most effective security programmes recognise the need for convergence, acknowledging that comprehensive information protection must address both the digital and physical domains in which information resides.

OUR KEY TIPS FOR SMES

Small and medium-sized enterprises (SMEs) face increasingly complex challenges in the digital operating environment. They are expected to maintain the same level of data protection as large organisations, but available resources are often limited. In this situation, it is important to understand the difference between information security and cybersecurity so that scarce resources can be allocated as effectively as possible. Information security covers all protection of company information regardless of whether the information is in digital, physical or human form. This includes, for example, customer registers, financial data, business processes and employees' tacit knowledge.

Cybersecurity, on the other hand, focuses on methods of protection against digital threats, such as firewalls, malware prevention and securing network infrastructure. Although SMEs often do not have the opportunity to maintain their own information security team, they can still achieve a high level of security through a strategic approach. We recommend a strategy for SMEs that addresses both domains through the following measures:Regarding information security, SMEs should create clear policies for data handling, classify sensitive information, implement basic physical protective measures and provide regular awareness training for all staff. These measures do not require large investments but can significantly reduce exposure to common threats.

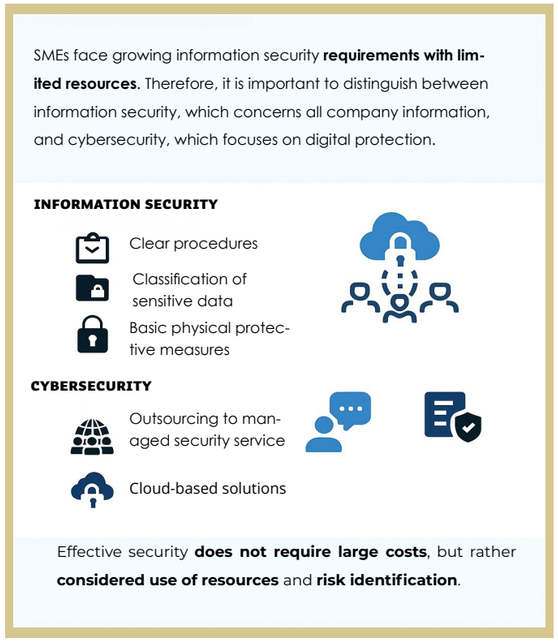
- Regarding information security, SMEs should create clear policies for data handling, classify sensitive information, implement basic physical protective measures and provide regular awareness training for all staff. These measures do not require large investments but can significantly reduce exposure to common threats.

- For cybersecurity, selective outsourcing to managed security service providers (MSSPs) may prove to be the most cost-effective option. External specialists can provide enterprise-level protection, continuous monitoring and rapid response to threat situations at a fraction of the cost of an internal team. SMEs should choose service providers who understand sector-specific requirements and can support compliance.

- Cloud-based security solutions offer a cost-effective means of improving protection. Subscription-based models enable access to advanced technologies without significant initial investments. Additionally, collaboration with security consultants can bring valuable insight and ensure regular assessment. For example, quarterly or half-yearly reviews can provide ongoing oversight without permanent staffing costs.

- Cybersecurity insurance complements technical and organisational measures by providing financial protection against damage. However, it is important for SMEs to ensure that the insurance covers their specific risks and operating environment.

As the measures demonstrate, effective information and cybersecurity does not necessarily require significant financial resources. Instead, it requires careful allocation of available resources based on a clear understanding of the organisation's risks. By separating information security and cybersecurity requirements, SMEs can develop their controls in the right proportion, which protects the business without significant costs. The best approach combines selective outsourcing and internal capability development. By training existing staff in security fundamentals, sustainable expertise can be built that strengthens the organisation's ability to operate independently and critically evaluate the work of external partners.



WHAT ABOUT VULNERABILITY MANAGEMENT FRAMEWORKS?

Vulnerability Management Frameworks in cybersecurity are structured approaches for identifying, evaluating, prioritising, and addressing security weaknesses in an organisation's systems and software. These frameworks establish consistent processes for managing security risks. By implementing vulnerability management frameworks, an SME can:

- detect vulnerabilities through regular scans, testing, and monitoring
- assess the severity and potential business impact of each vulnerability
- prioritise risks based on their magnitude, exploitability, and business implications
- support the tracking of remediation processes
- ensure that vulnerabilities are addressed appropriately
- enable clear reporting on the status of vulnerabilities across the entire organisation

Among the most widely recognised vulnerability management frameworks are the NIST Framework (particularly SP 800-40), CIS Controls, ISO/IEC 27001/2 standards, and the OWASP standards for web applications. These frameworks provide proven methods for reducing an organisation's attack surface and maintaining a strong security posture—even as new threats emerge. For SMEs with limited resources, these frameworks can be adapted in a more lightweight manner, focusing on the most critical systems. Even in this streamlined form, they offer a systematic defence against evolving cyber threats.

MOST COMMON VULNERABILITIES IN SUPPLY CHAINS

When discussing vulnerability management, it is clear that supply chain vulnerabilities cannot be overlooked. Cybersecurity is only as strong as its weakest link—and much like people, the supply chain often represents a critical point of weakness. When an SME uses external suppliers, subcontractors, or third-party software components, its attack surface expands significantly.

1. **Software components:** Open-source libraries and third-party components may contain vulnerabilities that are inherited by the end product.
2. **Supplier System Access**: External suppliers may have access to an organisation's critical systems and data, increasing risk if the supplier's security is inadequate.
3. **Hardware Vulnerabilities**: Device firmware or components may contain backdoors or vulnerabilities from the manufacturing stage.
4. **Update and Distribution Channel Attacks**: Attackers may target software update mechanisms to contaminate otherwise trusted software.

Particularly difficult to detect are so-called upstream vulnerabilities—such as when a software library depends on another library that itself contains a vulnerability. This kind of issue can be extremely complex to trace, and sometimes nearly impossible to identify, because the problem lies deep in the supply chain.

> **“ The zero trust philosophy should extend to encompass suppliers and external systems ”**

To protect your business against supply chain vulnerabilities, a multifaceted approach is essential. Begin by conducting regular supplier security assessments, incorporating thorough audits and embedding specific security requirements directly into your contracts. As part of your development process, it can come useful to implement comprehensive code reviews and vulnerability scanning to thoroughly examine third-party components before they enter your systems.

And now that you're at it, the zero trust philosophy should extend beyond your internal operations to encompass suppliers and external systems, ensuring that everyone operates under the principle of least privi lege. Understanding your complete supply chain landscape is equally important; through detailed mapping of all dependencies and suppliers, you'll gain visibility into potential weak points that might otherwise remain hidden.

This knowledge, coupled with the ability to deploy updates rapidly when vulnerabilities are detected, forms a robust defence strategy against increasingly sophisticated supply chain attacks that target the interconnected nature of modern business ecosystems.

For SMEs worried about supply chain security risks, we know that can be nearly impossible to map your whole supply chain, but you can begin with byt starting to make a simple checklist of security questions for all your vendors and partners. We also recommend you to regularly update all your software and check that your suppliers are doing the same - this simple step prevents most security problems before they can affect your business.

TO REMEMBER ABOUT SUPPLY CHAIN VULNERABILITIES

Supply chains often represent the weakest link in cybersecurity. Relying on external suppliers significantly expands the potential attack surface.

1. **Software Components:** Third-party components may harbour vulnerabilities that compromise system security.
2. **Supplier System Access:** External partners may gain unauthorised access to critical systems and sensitive data.
3. **Hardware Vulnerabilities:** Physical devices may contain deliberate backdoors or unintentional security flaws.
4. **Update and Distribution Channels:** Attackers can compromise software update mechanisms to distribute malicious code.

Effective protection requires a comprehensive, multi-layered approach:

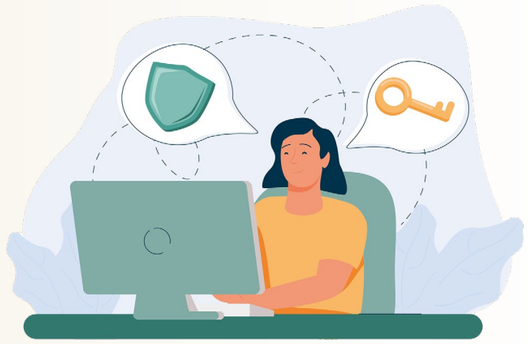
- Conducting regular security assessments of all suppliers
- Implementing zero-trust principles across all partnerships
- Maintaining detailed inventories of dependencies and supplier relationships

BUILDING A COMPREHENSIVE SECURITY FRAMEWORK OUT OF NOTHING

To further strengthen security, companies should employ **intrusion detection** and prevention systems that **monitor and respond to unauthorised access** attempts. These systems act as sentinels, alerting security personnel to suspicious activities and potentially blocking them automatically. Even organisations with limited IT resources can implement basic monitoring solutions that provide essential visibility into potential security incidents.

Regular security testing, such as **penetration testing**, helps **identify vulnerabilities** before they can be exploited. These proactive assessments simulate real-world attack scenarios to uncover weaknesses in systems and processes. While comprehensive penetration testing may require external expertise, smaller organisations can benefit from simplified **vulnerability scanning tools** and security checklists tailored to AI implementations.

In addition, **clear procedures** should be established for handling **denial-of-service** attacks, security breaches, and other incidents. This incident response planning ensures that organisations can react swiftly and effectively when security events occur, minimising damage and recovery time. **Documented procedures**, even if straightforward, **provide valuable guidance** during the stress of an actual security incident.



It is also important to note that the **biggest cybersecurity risk is you**. According to research from the World Economic Forum's Global Risks Report (2022), **roughly 95% of security issues involve some form of human mistake**. These mistakes take many forms – employees falling for phishing scams, creating passwords that are too simple, or mistakenly sending confidential information to unintended recipients. Such lapses can undermine even the most sophisticated security systems an organisation has in place.

Because human error and **social engineering attacks remain significant risks**, companies should also implement **training and safeguards** to mitigate these threats. Regular awareness training helps staff recognise and resist manipulation attempts such as phishing emails or pretexting calls. For SMEs where technical expertise is limited, focusing on human factors in security can yield significant protective benefits with relatively modest investment.

WHAT CAN SMES DO IF A DATA BREACH OCCURS?

Having a predefined incident response plan significantly reduces response time and potential damage from a breach. Even a straightforward document outlining key responsibilities and actions can prove invaluable during a security incident. If your small or medium-sized enterprise suffers a data breach, swift action is essential.

HERE ARE EIGHT CRITICAL STEPS TO TAKE DURING THIS EMERGENCY SITUATION:

1. **Contain the breach** by disconnecting affected systems from your network to prevent further data loss and damage.

2. **Assess the damage** by identifying what data was compromised, how the breach occurred, and who might be affected.

3. **Notify relevant authorities** according to regulations. In Finland and the EU, GDPR requirements mandate reporting significant breaches to authorities within 72 hours.

4. **Communicate with affected stakeholders**, including customers, partners, and employees whose data may have been compromised.

5. **Document everything** throughout your response process for regulatory compliance and insurance purposes.

6. **Address vulnerabilities** that led to the breach by patching systems or updating security protocols.

7. **Consider engaging professionals**, such as cybersecurity consultants or legal experts, if the breach is serious.

8. **Review and improve** your security practices based on lessons learned from the incident.

Remember that preparation is your strongest defence. A well-rehearsed plan enables your team to respond calmly and methodically when facing a crisis, rather than making hasty decisions under pressure, turn potential chaos into controlled action.

INTEGRATING CYBERSECURITY INTO THE BUSINESS

For all companies operating internet-facing services or internal tools — whether AI-based or not — cybersecurity must remain a constant priority. This typically includes a combination of staff training, structured security checklists, adherence to best coding practices, use of cybersecurity frameworks and specialised software, as well as regular audits and process reviews.

Organisations with limited technical resources can meet these demands effectively by combining outsourcing, cloud-based security solutions, and targeted internal initiatives. Security frameworks such as the NIST Cybersecurity Framework offer structured guidance that can be scaled to an organisation's size and complexity. Similarly, cloud service providers now offer increasingly advanced security tools that require minimal technical expertise to deploy.

AI itself plays a critical role in both strengthening and threatening cybersecurity. Managing security risks in AI development projects should begin early to avoid costly surprises in later deployment phases. This "security-by-design" approach embeds protective measures throughout the development lifecycle, rather than attempting to add them retrospectively — a strategy that is typically both more effective and more economical.

> **But I don't have any sensitive data, do I?** Did you know that under the General Data Protection Regulation (GDPR), all information related to individuals qualifies as personal data? If you have customers and/or employees, then you also have sensitive data that falls under GDPR regulations.

At the same time, malicious actors are leveraging AI to create increasingly sophisticated cyberattacks, while cybersecurity tools are using AI to detect and neutralise threats more efficiently. This technological arms race makes continuous cybersecurity awareness especially vital for organisations implementing AI solutions. Understanding both the protective capabilities and potential vulnerabilities of AI technologies helps you make informed decisions about their deployment and security.

THE GROWING IMPORTANCE OF INTEGRATION SECURITY IN THE AGE OF AI

As cyber threats continue to proliferate, the security of integrations has emerged as a critical concern for organisations across all sectors. The increasing reliance on APIs for processing sensitive data makes securing these connections paramount. Integration vulnerabilities or data breaches can result in severe operational disruption and reputational damage.

Furthermore, evolving regulations such as NIS2 and DORA are intensifying compliance pressures. Consequently, SMEs must demonstrate heightened vigilance regarding cybersecurity, both to safeguard against emerging threats and to ensure regulatory adherence. The question is not whether your business will face these challenges, but how well-prepared you will be when they arise.

KEY CONSIDERATIONS

Integration and cybersecurity teams are required to address fundamental questions:

- Are our integration implementations and platforms adequately secured?
- Do our developers consistently follow secure coding practices?
- Are our operational frameworks compliant with current regulatory requirements?

Take a moment to consider the next questions: how is your organisation addressing these critical questions? Do you fully comprehend their implications? Are your insights into regulatory requirements current and comprehensive?

COMMON AREAS REQUIRING STRENGTHENING

Whilst most SMEs today acknowledge these risks, many still require systematic support in addressing them effectively. The areas most commonly requiring reinforcement include:

- **Platform hardening:** Securing integration platforms against vulnerabilities
- **Secure development lifecycle:** Ensuring robust security practices throughout development and deployment
- **Proactive monitoring:** Implementing comprehensive logging and monitoring for early threat detection
- **Governance frameworks:** Establishing clear accountability models for integration security

Our Recommended Approach: By reinforcing the confidentiality, integrity, and availability of integrations and API interfaces, SMEs can respond more effectively to evolving cyber threats. With cyber risks continuing to escalate, assessing and strengthening integration security practices has become a strategic imperative—one that demands continuous attention and investment.

TOP5 BUDGET-FRIENDLY CYBERSECURITY TACTICS FOR SMALL BUSINESSES

1. CREATE A HUMAN FIREWALL THROUGH TARGETED TRAINING

Rather than implementing generic security awareness programmes, develop targeted training focused on your specific business vulnerabilities. Create scenario-based exercises that simulate real attacks your employees might encounter, including AI-powered phishing attempts that mimic your communication style. Designate “security champions” within each department who receive additional training and serve as first responders for security questions. This human-centric approach transforms security from an IT concern to a company-wide responsibility without requiring significant financial investment. Record measurable improvements by conducting simulated phishing tests before and after training to demonstrate ROI and refine your approach. Free tools can provide resources specifically designed for small businesses without dedicated security teams.

2. ADOPT ZERO TRUST ARCHITECTURE

Instead of relying solely on perimeter defences, implement a zero trust approach — "never trust, always verify" — gradually across your organisation. Start with practical, cost-effective steps: segment your network to isolate critical systems, enforce strict access controls based on clearly defined user roles, and require multi-factor authentication for sensitive resources. Each measured improvement significantly reduces your vulnerability without demanding enterprise-level security investments. And remember that different data requires different levels of protection. Begin with your most sensitive data and systems, including any AI applications processing customer information. This strategy focuses on verifying every user and device before granting access, regardless of location. Remember to adhere to data minimization principles, only collect and retain what’s essential for your operations.

3. LEVERAGE AI-POWERED SECURITY TOOLS DESIGNED FOR SMES

Turn AI to your advantage by utilising security tools that use machine learning to provide enterprise-grade protection at SME prices. Many cybersecurity vendors now offer AI-powered solutions specifically scaled for small businesses, with pricing models that accommodate limited budgets. Look for consolidated security platforms that combine multiple functions (antivirus, firewall, email protection) in one solution to maximise value. These tools can automatically detect unusual patterns that might indicate compromises, identify vulnerabilities before they’re exploited, and adapt to emerging threats — capabilities once available only to SMEs with dedicated security operations centres. Cloud security services are also a valuable option to consider, depending on your required level of security.

4. ESTABLISH A RISK-BASED SECURITY ROADMAP WITH CLEAR PRIORITIES

Develop a prioritised security roadmap based on business risk rather than attempting to implement comprehensive security all at once. Begin with a simple risk assessment identifying your crown jewels—the data and systems that would cause the most damage if compromised. Create a three-tier implementation plan focusing first on critical protections for your highest-value assets, then expanding protection as resources permit. This strategic approach ensures your limited security budget protects what matters most. Revisit and update this assessment quarterly as your business and the threat landscape evolve, particularly as you integrate new AI technologies. Even with limited resources, every SME should have a basic plan for handling security incidents. This doesn’t require sophisticated technology — just clear documentation of who is responsible for what actions when a breach occurs.

5. FORM STRATEGIC SECURITY PARTNERSHIPS AND POOL RESOURCES

Consider forming security cooperatives with other small businesses in your industry or region to share costs and expertise. This might include jointly retaining security consultants, sharing threat intelligence, or negotiating group rates for security services and training. Many industry associations also offer cybersecurity resources specifically tailored to their members’ needs. Don’t forget that Finland has a strong culture of collaboration in cybersecurity, with numerous free resources available to small and medium-sized businesses. These partnerships provide access to expertise and resources that would be unaffordable individually. By focusing on these strategic approaches rather than attempting to match the security capabilities of larger organisations, SMEs can develop effective protection for their data and systems—including AI applications—without breaking their budgets. Effective security is about smart implementation rather than complete coverage. Even modest, well-targeted investments can significantly reduce your most critical risks. For information on Finnish options, see the end of this document.

SUMMARY OF TOP 5 STRATEGIES FOR SMES

1. Build a Human Firewall: Create targeted security training with scenario-based exercises and designated security champions in each department.

2. Implement Zero Trust Gradually: Start with your most sensitive data and AI systems using the "never trust, always verify" principle.

3. Leverage AI-Powered Security Tools: Choose consolidated security platforms that use machine learning to provide enterprise-grade protection at SME prices.

4. Prioritise Based on Risk: Develop a tiered security roadmap that protects your most valuable assets first based on business impact.

5. Form Strategic Partnerships: Share security costs and expertise with other small businesses through cooperatives or industry associations.

HOW TO INTEGRATE CYBERSECURITY IN AI PROJECT IN SME

In today's rapidly evolving technological landscape, artificial intelligence offers tremendous opportunities for businesses of all sizes. However, as organisations with limited technical resources venture into AI implementation, cybersecurity considerations often remain an afterthought—a situation that can lead to serious consequences.

Cybersecurity encompasses measures that prevent malicious actors from gaining unauthorised access to data, taking control of systems, or disrupting operations. For SMES exploring AI solutions, the stakes are particularly high, as these organisations often lack dedicated security personnel yet may handle sensitive information through their AI applications.

The integration of AI technologies introduces unique security challenges. These systems typically process large volumes of data, making them attractive targets for cyber criminals. Moreover, AI applications often require connectivity to various data sources and networks, expanding the potential attack surface. This complexity necessitates a structured approach to security that begins with foundational understanding and extends to specific protective measures.

AI applications often require connections to various data sources and networks, which broadens the potential attack surface.

Ensuring security in AI-related projects requires attention to multiple aspects. User input should always be sanitised to prevent unintended commands from being executed. This validation process is critical for AI systems that interact with users through interfaces such as chatbots or data entry forms. Without proper sanitisation, these interactions could become vectors for malicious code injection.

Strong access control mechanisms must be in place to regulate both information access and operational permissions. This principle of least privilege ensures that users and system components can only access the data and functions necessary for their legitimate purposes. For AI systems that may process confidential business information or personal data, these controls serve as a primary defence against unauthorised data exposure.

Data security should be ensured through encryption protocols that protect information during transmission and storage. Encryption transforms readable data into coded information that requires a decryption key to access, making it significantly more difficult for attackers to exploit stolen information. For organisations implementing AI solutions that process sensitive data, encryption is not merely a technical best practice but often a regulatory requirement.

Systems must also be secured against SQL injection and other command injection attacks. These vulnerabilities can allow attackers to manipulate databases and execute unauthorised commands through seemingly innocent input fields. This is particularly relevant for AI systems that interface with databases containing valuable data.

To support your efforts in strengthening cybersecurity, numerous resources are available, including introductory courses, simplified frameworks, and managed security services designed specifically for smaller organisations. With appropriate attention to security considerations from the outset, companies of all technical capabilities can safely harness the transformative potential of artificial intelligence while protecting their valuable digital assets.

WHAT IS PHISHING EMAIL?

A phishing email is a fraudulent message designed to trick recipients into revealing sensitive information, such as passwords, financial details, or personal data. These emails often appear to come from trusted sources, such as banks, colleagues, or service providers, and may include urgent requests, fake links, or malicious attachments. The goal is to deceive the recipient into clicking a harmful link, downloading malware, or providing confidential information. To protect against phishing, always verify the sender, check for unusual language or formatting, and avoid clicking on suspicious links or attachments.

STILL NO STRATEGY? BEGIN BUILDING YOURS TODAY

In today's rapidly evolving digital landscape, a robust cybersecurity strategy has become an absolute necessity rather than a luxury. Cyberattacks are increasing in both sophistication and frequency, with businesses of all sizes finding themselves squarely in the crosshairs. The stakes are considerable, encompassing financial losses, reputational damage, legal ramifications, and the potential compromise of sensitive data. A single data breach can bring an entire organisation to its knees, with far-reaching consequences that may persist for years to come.

A well-designed cybersecurity strategy serves as the primary bulwark against such threats, safeguarding business continuity whilst protecting the trust painstakingly built with customers and partners. However, an effective strategy extends far beyond merely preventing attacks. It involves cultivating a security-conscious culture throughout the organisation, equipping employees with the knowledge and tools necessary to identify and respond to threats, thereby significantly reducing the risk of human error—a critical factor in numerous breaches. Given the increasing reliance on digital systems, cloud services, and remote working arrangements, every company must embrace a proactive approach to securing its data and infrastructure.

Failure to do so can result in substantial financial losses, legal liabilities, and irreparable damage to one's brand reputation. As global data protection and cybersecurity regulations such as the GDPR become increasingly stringent, businesses must ensure they satisfy all legal requirements.

> **An Investment That Pays Off:**
>
> Cybersecurity strengthens customer trust, protects your business operations, and provides peace of mind — allowing you to focus on growth without the constant fear of cyber threats.

An effective cybersecurity strategy guarantees that your organisation remains not only protected but also compliant, thereby avoiding hefty fines and penalties. Cybersecurity is therefore an investment that invariably yields returns: it strengthens customer confidence, protects operational integrity, and provides peace of mind, enabling you to concentrate on growth without the perpetual anxiety of cyber threats.

DEVELOPING AN EFFECTIVE SECURITY STRATEGY

To develop an effective cybersecurity strategy, it helps to break it down into several key areas. This section outlines the essential components that can offer immediate improvements to your organisation's data and cybersecurity posture.

1. DATA ENCRYPTION

- **Encryption at Rest:** Ensure that all sensitive data is encrypted while stored. Use AES-256 encryption — a robust and widely recognised standard — commonly applied in databases, file systems, and cloud storage.
- **Encryption in Transit:** Use TLS (Transport Layer Security) for any data transmitted across networks (e.g. HTTPS, SFTP, VPNs). Ensure that all APIs, communication channels, and network traffic are encrypted to defend against man-in-the-middle (MitM) attacks.
- **End-to-End Encryption (E2EE):** Implement E2EE for user-to-user communications, especially for email, chat, and file-sharing systems (e.g. using protocols from Signal or ProtonMail).

2. PACCESS CONTROL AND AUTHENTICATION

- **Multi-Factor Authentication (MFA):** Require MFA on all user accounts to add an additional layer of protection beyond passwords. No one should be exempt.
- **Role-Based Access Control (RBAC):** Apply least-privilege principles by ensuring users only have access to the information and systems necessary to perform their duties.
- **Regular Audit Logs:** Continuously monitor user access to systems and data. Store logs in tamper-resistant systems and review them regularly for suspicious activity.
- **Password Policies:** Enforce strong passwords (e.g. minimum of 12 characters including alphanumeric and special symbols) and mandate regular password updates.

3. NETWORK SECURITY

- **Firewall Configuration:** Use both software and hardware firewalls to regulate incoming and outgoing traffic based on security policies. Segment your network into zones (internal, external, DMZ) to reduce risk.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** Implement IDS/IPS to monitor network traffic for unusual patterns or indicators of attack.
- **Virtual Private Network (VPN):** Ensure remote employees access internal systems only via VPNs with strong encryption (e.g. OpenVPN or WireGuard).
- **Zero Trust Architecture:** Adopt the Zero Trust model, as previously discussed. This approach assumes no user, device, or network is inherently trusted — everything is treated as a potential risk.

4. ENDPOINT SECURITY

- **Antivirus and Anti-Malware:** Install up-to-date antivirus software on all devices to detect and eliminate threats. Consider using Endpoint Detection and Response (EDR) tools for continuous monitoring.
- **Device Encryption:** Enable full-disk encryption on all company laptops and mobile devices to prevent data exposure in the event of loss or theft (e.g. via BitLocker or FileVault).
- **Mobile Device Management (MDM):** Implement MDM solutions to ensure all company devices are secured, monitored, and can be remotely wiped if compromised.

PRINCIPLE OF LEAST PRIVILEGE?

The principle of least privilege means that users and processes are granted only those access rights which are absolutely essential for carrying out their tasks. This principle helps to minimise the impact of security breaches and prevent vulnerabilities.

5. DATA LOSS PREVENTION (DLP)

Use DLP software to monitor and restrict unauthorised sharing or export of sensitive data. This helps prevent data breaches caused by internal threats or accidental disclosures.

6. CLOUD SECURITY

- **Encryption in Cloud Services:** Ensure your cloud service provider supports encryption for both data at rest and in transit. Use client-side encryption wherever possible to retain control over encryption keys.
- **Secure API Integrations:** Make sure all APIs used in cloud service integrations are secured and monitored for abnormal behaviour.
- **Backups and Disaster Recovery:** Implement regular, encrypted backups of all critical data and maintain a disaster recovery plan to restore systems in the event of an attack.

7. INCIDENT RESPONSE PLANNING

Develop an incident response plan (IRP) for the rapid detection, response, and recovery from cyberattacks. Your IRP should include:

- Clearly defined roles and responsibilities
- Procedures for identifying, containing, and mitigating attacks
- Post-incident review and lessons learned

Regularly test your IRP through simulations or tabletop exercises.

8. STAFF TRAINING AND AWARENESS

- Conduct regular training sessions on phishing, password security, and data handling best practices.
- Implement phishing simulation programmes to help employees identify and avoid phishing attempts.
- Establish clear policies outlining acceptable device use, data handling procedures, and how to report suspicious activity.

9. THIRD-PARTY VENDOR SECURITY

- Conduct thorough security assessments of all third-party vendors.
- Require security certifications (e.g. SOC 2, ISO 27001) and ensure they comply with your company's security policies.
- Draft strong Data Processing Agreements (DPAs) to guarantee that all third-party processors adhere to regulatory standards such as GDPR.

10. REGULATORY COMPLIANCE

Ensure compliance with relevant regulations (e.g. GDPR, HIPAA). Carry out regular audits and assessments to remain aligned with applicable standards.

By addressing each of these areas with appropriate solutions, you can build a comprehensive cybersecurity strategy tailored to your organisation's specific needs.

KEY QUESTIONS

These questions can serve as a self-assessment tool, a conversation starter in your training sessions, or a support framework during planning phases of your AI projects.

INITIAL ASSESSMENT:

- Do you have dedicated **IT security personnel**, or is everyone responsible?
- What types of **sensitive data** do you process through your **AI applications**? Make a list of the **data categories** involved in your AI systems.
- How well do you understand the **unique security challenges** presented by **AI technologies**? Does your organisation have **prior experience** in this area?

TECHNICAL SAFEGUARDS:

- How do you ensure that **user inputs are validated and sanitised** before being processed? What mechanisms are in place?
- Do your users **operate under robust access control systems** based on the **principle of least privilege**?
- Are the data you manage adequately **encrypted during storage** and **transmission**? And do these methods meet **legal and regulatory requirements**?
- How do you prevent **SQL injection** and other **command injection attacks** in chatbots, forms, and other user interfaces or systems?

RISK MANAGEMENT:

- How extensive is your organisation's **attack surface** due to **AI system connectivity and other integrations**?
- Do your AI systems contain **large volumes of data**? Could this make your systems **attractive targets** for cybercriminals?
- Are you aware of **all the sources your AI systems draw data from**, and how are these sources secured?
- What **serious consequences** could result from **security shortcomings**? And what impact could a **data breach** have on your customers?

RESOURCES AND SUPPORT:

- What **cybersecurity resources** designed for SMEs could you take advantage of?
- Do you require **outsourced security services**, or do you manage your SMEs security internally? Do you have external providers in your network?
- How do you **integrate security considerations** into your AI projects from the design phase? And how do you ensure they are **followed throughout** the project lifecycle?

STANDARDS, REGULATIONS, AND OTHER ACTIVITIES:

- What **legal obligations** apply to your data processing?
- Do your encryption methods comply with those **legal standards**?
- Do you have a **systematic cybersecurity framework** or model in place to support your AI initiatives and wider operations?
- How are you **preparing for cyberattacks**, and how quickly could you **recover** from a potential breach?

We hope this set of questions proves useful to you and your organisation. Remember, adopting AI is a strategic investment that demands responsible and secure implementation. Companies that incorporate cybersecurity from the earliest stages of their projects not only protect themselves from risk but also strengthen their competitive position in a market where trust and data protection are increasingly vital.

By embedding security into your AI strategy from the outset, your business can confidently embrace the opportunities of AI — boldly and sustainably.

FOOD FOR THOUGHT

When you get into a car, you fasten your seatbelt. When you leave home, you lock your doors and windows. We rarely think twice about these actions because they've become second nature. When you take medicine, you read the patient information leaflet. When you buy insurance, you carefully review the terms and conditions. When you open a bank account, you sign a contract knowing exactly what you're agreeing to. These are natural precautions we follow in the physical world – we have no choice.

But why, then, do we often show such indifference towards our digital doors and windows? Why are we prepared to risk outsiders intruding into our digital privacy? Why do we blindly accept terms and conditions without reading them at all, surrendering our personal data to companies whose business practices we know virtually nothing about? Every search we make online, every purchase, every message we send is collected, analysed, and stored.

Our data has become the new oil, but unlike actual oil reserves, we often don't know who's extracting it, how it's being used, or what it's truly worth. Whilst we demand detailed ingredient lists on food products, we give digital services carte blanche to collect every possible piece of information about our lives. Companies hold vast amounts of sensitive information about their customers, employees, and partners. National insurance numbers, banking details, health records, location data, and communications – all this information flows through corporate networks daily.

When a company collects data, it accepts responsibility for protecting it in the same way a bank is responsible for the contents of its vault or a hospital for its patient records. Secure data handling isn't merely a technical consideration – it's a fundamental aspect of corporate social responsibility. In this sense, a data breach doesn't just harm the company itself – it can destroy customers' lives for years to come, as the Vastaamo case demonstrated. Personal data falling into the wrong hands can lead to identity theft, financial losses, blackmail, and even threats to personal safety.

This is why companies must build digital security into the very foundation of their business operations – not merely as a technical requirement, but as a moral obligation to protect the lives of all those who have entrusted them with their most sensitive information.

You too must prove worthy of that trust.

USEFUL LINKS (2025)

A comprehensive ecosystem of cybersecurity support exists to help organisations of all sizes: accessible training courses, streamlined operational frameworks, and managed security services designed specifically for smaller enterprises. By embedding cybersecurity into their foundations from day one, businesses, regardless of their technical expertise, can confidently embrace transformative technologies like artificial intelligence whilst safeguarding their digital assets.

FREE LEARNING MATERIALS

- MinnaLearning: Cybersecurity - A beginner's guide (comprehensive online course developed with the EU Digital SkillUp Initiative)
- Confederation of Finnish Industries (EK): Cybersecurity Essentials for Business (practical webinar materials covering fundamental protection strategies in Finnish)
- W3 Schools: Cyber Security Tutorial (accessible collection of cybersecurity fundamentals)
- National Cyber Security Centre Finland: Enterprise Security Resource (several guides and comprehensive materials for larger operations)
- Finnish Government NIS2 Implementation Guide: NIS2 Directive strengthens cybersecurity across the EU – National implementation launched in January (press release)
- Synopsys: Glossary Key Terms (vocabulary for cybersecurity)

PROFESSIONAL DEVELOPMENT

Established training organisations including Tieturi and Aalto Executive Education offer structured cybersecurity programmes ranging from executive briefings to technical certifications. Universities such as Aalto University and University of Jyväskylä, alongside universities of applied sciences including XAMK, Laurea, and JAMK, provide degree programmes in cybersecurity and related disciplines. It's also worth of checking the certifications.

- Finnish Cyber Security Certificate: Nationally recognised professional credential
- ISO: ISO/IEC 27002:2022 (international information security management standards)

REGULATORY ENVIRONMENT

Cybersecurity governance operates within a multi-layered regulatory framework encompassing dedicated national and EU legislation, alongside cybersecurity provisions embedded within broader legal instruments such as the Finnish Criminal Code. These regulations establish clear accountability structures and define stakeholder responsibilities for maintaining robust digital security postures.

The regulatory landscape is complemented by industry standards, certification programmes, and specialised agencies such as ENISA (the European Union Agency for Cybersecurity). For a comprehensive introduction to this complex field, the EU's cybersecurity policy overview provides an excellent starting point.

- European Comission: European Commission Cybersecurity Policy Overview (strategic context and regulatory landscape)
- European Comission: NIS2 Directive: securing network and information systems (information on the directive that tightens cybersecurity requirements for businesses and public authorities)
- Traficom: Cyber security and the responsibilities of boards (guide book)
- ENISA: European Union Agency for Cybersecurity (website)
- CRA: European Cyber Resilience Act (information package)

PRACTICAL SUPPORT SERVICES

These represent a sample of providers. We recommend conducting thorough research to identify services that align with your organisation's specific requirements and budget.

- Robocoast EDIH: Test Before Invest Services (comprehensive device and system security testing (€675 per consultant day + VAT))
- Centria: Centria SecuLab (continuous and reliable security and data protection services)
- JAMK: Cybersecurity Services (courses, trainings and testings)
- JAMK: JYVSECTEC (different services and information)

PROFESSIONAL ORGANISATIONS

- Finnish Information Security Cluster (FISC) - blogs, events and resources
- Tietoturva ry - The Finnish Information Security Association

SMALL GLOSSARY

To enhance your reading experience, we have compiled a glossary of technical terms used throughout this guide. We recommend reviewing these definitions before proceeding with the main content.

AES-256 (Advanced Encryption Standard): A robust encryption standard employing a 256-bit key for data encryption and decryption. As a symmetric encryption algorithm, it uses the same key for both encrypting and decrypting information, making it highly secure for protecting sensitive data.

API (Application Programming Interface): A set of protocols and specifications that enable seamless communication between different software applications or systems. Think of it as a digital contract that defines how applications can securely request, exchange, and receive data from one another.

DDoS Attack (Distributed Denial of Service): A coordinated cyber attack where multiple compromised devices simultaneously flood a target system—such as a website or server—with traffic, causing it to crash or become severely degraded. This prevents legitimate users from accessing the service.

DLP (Data Loss Prevention): A comprehensive security strategy designed to prevent unauthorised access, theft, or misuse of sensitive organisational data. DLP systems continuously monitor data usage, transfer, and storage to identify potential security breaches before they occur.

DORA (Digital Operational Resilience Act): EU regulation aimed at strengthening the digital operational resilience of financial services firms against cyber threats and operational disruptions. While primarily focused on operational resilience, it incorporates essential cybersecurity principles and practices.

E2EE (End-to-End Encryption): A security method where messages are encrypted on the sender's device and can only be decrypted by the intended recipient's device. This ensures that even if intercepted, the communication remains unreadable to unauthorised parties, including service providers.

Vulnerability Assessment: A systematic process of identifying, evaluating, and prioritising security weaknesses within systems or applications. The goal is to proactively address potential threats before they can be exploited by malicious actors.

Injection Attack: A cyber attack technique where malicious code or commands are inserted into vulnerable applications, websites, or databases. The objective is typically to gain unauthorised access, steal data, or compromise system integrity.

Integration Hardening: The process of securing and configuring integration platforms and solutions (including API gateways, data management systems, enterprise service buses, and cloud integration services) to minimise security vulnerabilities and reduce potential attack vectors.

Cryptography: The science of securing information through encryption and decryption techniques. Crypto graphy transforms readable data into an encoded format that only authorised parties with the correct decryption key can access, forming the foundation of modern digital security.

Logging: The automated process of recording system activities, user actions, and security events in chronological order. These digital records, known as logs, serve as an audit trail for troubleshooting system issues, monitoring performance, and investigating security incidents.

MFA (Multi-Factor Authentication): A layered security approach requiring users to verify their identity through multiple independent methods before gaining system access. Typically combines something you know (password), something you have (mobile device), and something you are (biometric data).

NIS and NIS2 (Network and Information Systems Directives): Progressive EU cybersecurity legislation establishing mandatory security requirements for operators of essential services and digital service providers. NIS2, the updated directive, expands coverage and strengthens incident reporting obligations to enhance collective cyber resilience across member states.

Penetration Testing: An authorised simulated cyber attack conducted by security professionals to evaluate system defences. Often called "ethical hacking," pen testing identifies exploitable vulnerabilities before malicious actors can discover and abuse them, providing organisations with actionable security improvements.

RBAC (Role-Based Access Control): An access management strategy that grants system permissions based on job functions rather than individual identities. Users inherit access rights appropriate to their organisational role, simplifying administration whilst enforcing the principle of least privilege.

Security by Design: A proactive development philosophy integrating security considerations throughout the entire product lifecycle, from initial concept to deployment. Rather than retrofitting security measures, this approach embeds protection mechanisms as core functional requirements from day one.

SQL Injection: A code injection attack targeting databases through vulnerable web applications. Attackers insert malicious SQL commands into input fields, potentially accessing, modifying, or deleting sensitive database information by exploiting insufficient input validation and query construction practices.

Input: Any data, commands, or signals provided to a computer system from external sources. This includes user interactions (keyboard input, mouse clicks), file uploads, network data, sensor readings, and any information processed by software applications.

TLS (Transport Layer Security): The cryptographic protocol securing internet communications by encrypting data in transit between clients and servers. TLS prevents eavesdropping, tampering, and message forgery, providing the security foundation for HTTPS websites, email, and other network services.

XSS Attack (Cross-Site Scripting): A web application vulnerability enabling attackers to inject malicious scripts into trusted websites viewed by other users. When victims visit the compromised site, the malicious code executes in their browsers, potentially stealing session cookies, redirecting to phishing sites, or performing unauthorised actions on their behalf.

ABOUT THIS GUIDE

This cybersecurity guide has been developed by Finnish AI Region (FAIR) – **your trusted partner in building a digital future**. FAIR provides Finnish small and medium enterprises with practical expertise across **artificial intelligence**, **augmented reality**, **high-performance computing**, and **cybersecurity**. Our complimentary services are designed to accelerate AI adoption and drive digital transformation in Finnish businesses.

WHY PARTNER WITH FAIR?

- World-class services with a low threshold
- Free expertise and testing services
- We focus on the real needs and challenges of SMEs
- A Finnish operator that understands the local business environment
- Bespoke services designed for real business impact

STRONG FUNDING BASE ENSURES QUALITY

FAIR's operations are made possible through the support of our stakeholders:

- European Commission – supporting digital transition
- Business Finland – strengthening the Finnish innovation ecosystem
- Helsinki Innovation Fund – supporting start-up and growth companies

EXPLORE OUR SERVICES

Explore our comprehensive suite of services and connect with our team. We're here to guide your business through its next phase of digital evolution.

ACKNOWLEDGEMENTS

This guide was written by **Martti Asikainen** (Haaga-Helia), **Solja Sulkunen** (Business Helsinki), **Jussi Rantsi** (Aalto & Helsinki University) and **Jenni Selosmaa** (City of Espoo). We extend our sincere gratitude to **Marie Skavø-Sinisalo** from South-Eastern Finland University of Applied Sciences (Xamk) for her invaluable insights and expert review of this guide.

FINNISH AI REGION IS

- Aalto University and University of Helsinki
- Haaga-Helia and Metropolia Universities of Applied Sciences
- Cities of Helsinki, Espoo, and Vantaa
- CSC – IT Centre for Science
- EIT Digital and KiraHUB
- Enter Espoo and Helsinki XR Center

OUR PARTNERS ARE

- ABB
- Arcada
- Google
- Microsoft
- Helsinki-Uusimaa Regional Council
- Varian Siemens
- FCAI
- Technology Industries of Finland

At Finnish AI Region, we're building a dynamic ecosystem that transforms how businesses embrace technology. We remain at the forefront of technological innovation, world-class research, and talent development.

Our mission centres on pioneering breakthrough innovations in digital services, healthcare, and smart cities. By connecting key stakeholders, we generate substantial value for Finland's economy and the broader European Union. FAIR creates tomorrow's opportunities whilst developing sustainable solutions for future challenges.

Discover our full range of services and partnership opportunities at:

https://www.fairedih.fi

FAIR
Finnish AI Region | EDIH

In our digital age, every business faces risks, but is also brimming with opportunities. This practical guide is specifically designed for small and medium-sized enterprises without dedicated IT departments, who wish to implement artificial intelligence safely and strategically.

The guide clarifies the distinction between cybersecurity and information security, whilst providing concrete, cost-effective solutions for strengthening your company's digital defences. By reading this guide, you'll gain clear instructions for secure AI implementation, an accessible framework for protecting your business, and practical tips for training your team to identify and counter threats.

Whether you're just beginning to explore AI or are already building new services around it, this guide will help you take the next step with confidence and responsibility. You don't need an IT background—simply the desire to develop your business intelligently and responsibly. Remember that cybersecurity doesn't require a large budget — just smart decisions.

FAIR
Finnish AI Region | EDIH

www.fairedih.fi
Co-funded by European Union