

Plain English Cybersecurity Glossary for SMEs

A free Aldermere Systems glossary for small businesses.

VERSION 1.0 | REVIEWED 5 AUGUST 2026 | COPYRIGHT (C) 2026 ALDERMERE SYSTEMS. ALL RIGHTS RESERVED.

Start Here

START HERE

MFA / 2FA

Stops many account takeovers, even when passwords leak.

START HERE

Cyber Essentials

Practical UK baseline for basic business cybersecurity.

START HERE

GDPR / UK GDPR

Applies when handling personal data.

START HERE

ICO

UK regulator for data protection and information rights.

START HERE

SPF

Helps reduce fake email pretending to come from your domain.

START HERE

DKIM

Helps prove outgoing email has not been tampered with.

START HERE

DMARC

Tells mail systems what to do when email authentication fails.

START HERE

Backups

Helps recover files and systems after mistakes, failure, or attack.

START HERE

MSP

Helps businesses understand what their IT provider actually does.

START HERE

API Key

Important when using AI tools, integrations, and connected software safely.

Glossary

CATEGORY

Business and General IT

USEFUL

BAU

Business As Usual

Normal day-to-day business operations.

ESSENTIAL

BCP

Business Continuity Plan

A plan for keeping the business running during disruption.

USEFUL

BYOD

Bring Your Own Device

Staff using their own phones, tablets or laptops for work.

USEFUL

CRM

Customer Relationship Management

Software used to manage customers, leads, sales and communication history.

ESSENTIAL

DR

Disaster Recovery

How a business restores systems and data after a major failure.

USEFUL

ERP

Enterprise Resource Planning

Software that manages major business processes like stock, accounts and operations.

USEFUL

HR

Human Resources

The people, payroll, hiring and staff management side of a business.

USEFUL

KPI

Key Performance Indicator

A number used to measure whether something is working well.

ESSENTIAL

MSP

Managed Service Provider

An outsourced IT company that looks after computers, networks, updates and support.

USEFUL

MSSP

Managed Security Service Provider

Like an MSP, but focused on cybersecurity monitoring and protection.

USEFUL

OEM

Original Equipment Manufacturer

A company that makes original parts, devices or software used in another company's product.

USEFUL

POS

Point of Sale

A till, checkout or payment system.

USEFUL

ROI

Return on Investment

Whether the money spent on a product or service gives enough value back.

ESSENTIAL

RPO

Recovery Point Objective

How much data loss is acceptable after a failure.

ESSENTIAL

RTO

Recovery Time Objective

How quickly a system needs to be restored after an outage.

USEFUL

SLA

Service Level Agreement

A promise about support response times, uptime or service quality.

USEFUL

SMB

Small and Medium-sized Business

Another way of saying SME, often used in software and IT sales.

USEFUL

SME

Small and Medium-sized Enterprise

A small or medium-sized business. Usually not a huge corporation, but big enough to need proper systems and security.

USEFUL

SOP

Standard Operating Procedure

A written step-by-step process for doing a task properly.

USEFUL

TCO

Total Cost of Ownership

The full cost of something over time, including setup, support, licences and maintenance.

Cybersecurity Basics

ESSENTIAL

2FA

Two-Factor Authentication

A type of MFA using two login checks.

ADVANCED

APT

Advanced Persistent Threat

A skilled attacker or group that stays hidden and targets organisations over time.

USEFUL

AV

Antivirus

Software that detects and blocks known malware.

ESSENTIAL

Backups

Not an acronym

Copies of important files and systems that can be restored after mistakes, failure, theft, or attack.

ADVANCED

CASB

Cloud Access Security Broker

Security controls placed between users and cloud services.

ADVANCED

CVE

Common Vulnerabilities and Exposures

A public reference number for a known software security weakness.

ADVANCED

CVSS

Common Vulnerability Scoring System

A score showing how serious a vulnerability is.

ADVANCED

DLP

Data Loss Prevention

Tools and rules that stop sensitive data being leaked or sent to the wrong place.

USEFUL

EDR

Endpoint Detection and Response

Security software that watches laptops, desktops and servers for suspicious activity.

USEFUL

FW

Firewall

A barrier that controls what network traffic is allowed in or out.

USEFUL

IAM

Identity and Access Management

Controlling who can log in, what they can access and what they can change.

ADVANCED

IDS

Intrusion Detection System

A system that spots possible attacks.

ADVANCED

IOC

Indicator of Compromise

A clue that a system may have been attacked, such as a bad IP address or suspicious file.

ADVANCED

IPS

Intrusion Prevention System

A system that can block possible attacks.

ADVANCED

MDR

Managed Detection and Response

A managed service where security experts monitor and respond to threats for you.

ESSENTIAL

MFA

Multi-Factor Authentication

Logging in with more than just a password, such as a code, app prompt or security key.

ADVANCED

NGFW

Next-Generation Firewall

A more advanced firewall with deeper inspection and security features.

ADVANCED

PAM

Privileged Access Management

Extra control over powerful admin accounts.

USEFUL

RBAC

Role-Based Access Control

Giving people access based on their job role.

ADVANCED

SIEM

Security Information and Event Management

A system that collects security logs and helps spot suspicious behaviour.

ADVANCED

SOAR

Security Orchestration, Automation and Response

Tools that automate parts of security investigation and response.

ADVANCED

SOC

Security Operations Centre

A team or service that monitors security alerts and incidents.

USEFUL

SSO

Single Sign-On

One login used to access multiple systems.

ADVANCED

TTP

Tactics, Techniques and Procedures

The methods attackers use.

ADVANCED

UTM

Unified Threat Management

A security appliance or service combining several protections in one place.

USEFUL

VPN

Virtual Private Network

A secure connection used to access systems remotely or protect network traffic.

USEFUL

WAF

Web Application Firewall

Protection for websites and web apps against common attacks.

ADVANCED

XDR

Extended Detection and Response

Security monitoring across multiple areas, such as devices, email, cloud and network.

ADVANCED

Zero-day

Zero-day Vulnerability

A security flaw that is being used before a fix is available.

CATEGORY

Common Cyber Threats

USEFUL

BEC

Business Email Compromise

A scam where criminals use email to trick staff into paying money or sharing information.

USEFUL

CEO Fraud

Chief Executive Officer Fraud

A scam where an attacker pretends to be the boss and asks for urgent payment or action.

ADVANCED

CSRF

Cross-Site Request Forgery

An attack that tricks a logged-in user's browser into performing an unwanted action.

USEFUL

DDoS

Distributed Denial of Service

A larger DoS attack using many devices at once.

USEFUL

DoS

Denial of Service

An attack that tries to make a website or system unavailable.

USEFUL

MITM

Man-in-the-Middle

An attack where someone secretly intercepts communication between two parties.

USEFUL

MITRE ATT&CK

MITRE Adversarial Tactics, Techniques and Common Knowledge

A knowledge base describing how cyber attackers operate.

USEFUL

OSINT

Open Source Intelligence

Information gathered from public sources such as websites, social media, records and search engines.

USEFUL

RAT

Remote Access Trojan

Malware that lets an attacker control a device remotely.

ADVANCED

RCE

Remote Code Execution

A serious flaw that lets an attacker run commands on a system from elsewhere.

ADVANCED

SQLi

SQL Injection

An attack where database commands are inserted into website forms or requests.

USEFUL

XSS

Cross-Site Scripting

A website attack where malicious script runs in a user's browser.

CATEGORY

Compliance, Governance and Standards

SECTOR-SPECIFIC

CAF

Cyber Assessment Framework

A framework used to assess cyber resilience, especially in regulated or essential services.

ESSENTIAL

CE

Cyber Essentials

A UK government-backed cybersecurity certification covering basic protective controls.

USEFUL

CE+

Cyber Essentials Plus

Cyber Essentials with independent technical testing.

SECTOR-SPECIFIC

CSR Bill

Cyber Security and Resilience Bill

UK legislation intended to update and strengthen cyber resilience rules.

USEFUL

DPA

Data Protection Act

UK data protection legislation that works alongside UK GDPR.

USEFUL

DPIA

Data Protection Impact Assessment

A risk assessment for projects that may affect people's privacy.

USEFUL

DPO

Data Protection Officer

A person responsible for advising on and monitoring data protection compliance.

USEFUL

DSAR

Data Subject Access Request

Another name for a Subject Access Request.

SECTOR-SPECIFIC

DSIT

Department for Science, Innovation and Technology

UK government department responsible for areas including digital, technology and cyber policy.

SECTOR-SPECIFIC

DSP

Digital Service Provider

A provider of digital services such as cloud, search or online marketplaces.

USEFUL

FOI

Freedom of Information

Rules allowing access to certain public authority information.

ESSENTIAL

GDPR

General Data Protection Regulation

Data protection law covering how personal data is handled.

SECTOR-SPECIFIC

IASME

Information Assurance for Small and Medium Enterprises

Organisation involved in Cyber Essentials delivery and SME-focused assurance.

ESSENTIAL

ICO

Information Commissioner's Office

The UK regulator for data protection and information rights.

USEFUL

ISMS

Information Security Management System

The policies, processes and controls used to manage information security.

USEFUL

ISO

International Organization for Standardization

An organisation that publishes international standards.

USEFUL

ISO 27001

Information Security Management Standard

A recognised standard for managing information security properly.

USEFUL

NCSC

National Cyber Security Centre

The UK's national technical authority for cybersecurity.

SECTOR-SPECIFIC

NIS

Network and Information Systems

UK/EU rules focused on security and resilience for important digital and essential services.

SECTOR-SPECIFIC

OES

Operator of Essential Services

An organisation providing important services such as energy, transport, water or healthcare.

SECTOR-SPECIFIC

PCI DSS

Payment Card Industry Data Security Standard

Security rules for organisations that handle card payments.

USEFUL

PECR

Privacy and Electronic Communications Regulations

UK rules covering electronic marketing, cookies and similar communications.

SECTOR-SPECIFIC

PHI

Protected Health Information

Health-related personal information, mainly used in healthcare contexts.

USEFUL

PII

Personally Identifiable Information

Information that can identify a person, directly or indirectly.

SECTOR-SPECIFIC

PPN

Procurement Policy Note

UK government procurement guidance for public sector buying.

USEFUL

RoPA

Record of Processing Activities

A record of what personal data an organisation processes and why.

USEFUL

SAR

Subject Access Request

A request from an individual asking what personal data an organisation holds about them.

ESSENTIAL

UK GDPR

United Kingdom General Data Protection Regulation

The UK version of GDPR after Brexit.

CATEGORY

Networking and Internet

USEFUL

DHCP

Dynamic Host Configuration Protocol

The system that automatically gives devices their network settings.

USEFUL

DNS

Domain Name System

The system that turns website names into IP addresses.

USEFUL

FTP

File Transfer Protocol

An older method for moving files between systems.

USEFUL

HTTP

HyperText Transfer Protocol

The basic protocol used by websites.

USEFUL

HTTPS

HyperText Transfer Protocol Secure

The secure version of HTTP, using encryption.

USEFUL

IP

Internet Protocol

The system used to send data across networks.

USEFUL

IP Address

Internet Protocol Address

A number that identifies a device on a network or the internet.

USEFUL

LAN

Local Area Network

A network inside a building or site.

USEFUL

MAC Address

Media Access Control Address

A hardware address used to identify a network device.

USEFUL

NAT

Network Address Translation

A method that lets many devices share one public internet address.

USEFUL

QoS

Quality of Service

Network settings that prioritise important traffic such as voice or video.

USEFUL

RDP

Remote Desktop Protocol

A way to remotely control a Windows computer.

USEFUL

SFTP

Secure File Transfer Protocol

A secure method for transferring files.

USEFUL

SSH

Secure Shell

A secure way to log in to and manage remote systems.

USEFUL

SSL

Secure Sockets Layer

Older term still commonly used for website security certificates.

USEFUL

TCP

Transmission Control Protocol

A reliable method for sending data over networks.

USEFUL

TLS

Transport Layer Security

The modern security technology behind HTTPS.

USEFUL

UDP

User Datagram Protocol

A faster, less strict method for sending network data.

USEFUL

VLAN

Virtual Local Area Network

A separated network created inside a larger network.

USEFUL

VoIP

Voice over Internet Protocol

Phone calls carried over the internet.

USEFUL

WAN

Wide Area Network

A network spread across multiple locations or the internet.

USEFUL

WLAN

Wireless Local Area Network

A Wi-Fi network.

CATEGORY

Email, Domains and Website Security

USEFUL

A Record

Address Record

A DNS record pointing a domain to an IPv4 address.

USEFUL

AAAA Record

IPv6 Address Record

A DNS record pointing a domain to an IPv6 address.

USEFUL

CDN

Content Delivery Network

A network that helps websites load faster and can add protection.

USEFUL

CMS

Content Management System

Website software such as WordPress, Shopify or similar platforms.

USEFUL

CNAME

Canonical Name

A DNS alias pointing one name to another.

USEFUL

CTA

Call To Action

A button or message asking the visitor to do something, such as "Buy Now" or "Contact Us".

ESSENTIAL

DKIM

DomainKeys Identified Mail

A system that digitally signs email to prove it was not altered.

ESSENTIAL

DMARC

Domain-based Message Authentication, Reporting and Conformance

A policy that tells mail systems what to do if SPF or DKIM checks fail.

USEFUL

MX

Mail Exchange

DNS records that tell the internet where email for a domain should go.

USEFUL

SEO

Search Engine Optimisation

Improving a website so search engines can understand and rank it.

USEFUL

SERP

Search Engine Results Page

The results page shown by a search engine.

ESSENTIAL

SPF

Sender Policy Framework

A DNS record that says which servers are allowed to send email for a domain.

USEFUL

TXT

Text Record

A DNS record often used for verification and email security settings.

USEFUL

UI

User Interface

The visible buttons, menus, screens and controls a user interacts with.

USEFUL

UX

User Experience

How easy and pleasant a website, app or system is to use.

CATEGORY

Cloud, Software and Development

USEFUL

API

Application Programming Interface

A way for software systems to talk to each other.

USEFUL

CD

Continuous Delivery or Continuous Deployment

Automatically preparing or releasing software updates.

USEFUL

CI

Continuous Integration

Automatically testing code when changes are made.

USEFUL

CLI

Command Line Interface

A text-based way to control software using commands.

USEFUL

CSS

Cascading Style Sheets

The styling language used for web pages.

USEFUL

CSV

Comma-Separated Values

A simple spreadsheet-style text file.

USEFUL

DB

Database

A structured place where information is stored.

USEFUL

DevOps

Development and Operations

A way of working that connects software development, deployment and operations.

USEFUL

DevSecOps

Development, Security and Operations

DevOps with security built into the process.

USEFUL

Docker

Container Platform

A tool for packaging software so it runs consistently.

USEFUL

Git

Git Version Control

A system for tracking changes in code and files.

USEFUL

GitHub

Git Hosting Platform

A platform used to store, review and collaborate on code.

USEFUL

GUI

Graphical User Interface

A visual interface with windows, buttons and menus.

USEFUL

HTML

HyperText Markup Language

The structure language used for web pages.

USEFUL

IaaS

Infrastructure as a Service

Cloud servers, storage and networking rented instead of owned.

USEFUL

IDE

Integrated Development Environment

Software used to write, test and manage code.

USEFUL

JS

JavaScript

A programming language commonly used for websites and apps.

USEFUL

JSON

JavaScript Object Notation

A common data format used by software and APIs.

USEFUL

Kubernetes

Container Orchestration Platform

A system for managing lots of containers.

USEFUL

MVP

Minimum Viable Product

The simplest working version of a product that proves the idea.

USEFUL

PaaS

Platform as a Service

A cloud platform for building or running applications.

USEFUL

SaaS

Software as a Service

Software used online, usually by subscription.

USEFUL

SDK

Software Development Kit

Tools and code that help developers build with a platform.

USEFUL

SQL

Structured Query Language

A language used to work with databases.

USEFUL

VM

Virtual Machine

A software-based computer running inside another computer.

USEFUL

VPS

Virtual Private Server

A rented virtual server, usually hosted in a data centre.

USEFUL

XML

Extensible Markup Language

An older structured data format still used by many systems.

USEFUL

YAML

YAML Ain't Markup Language

A human-readable configuration file format.

CATEGORY

AI and Automation

USEFUL

Agent

AI Agent

An AI system that can take steps toward a task, not just answer one question.

USEFUL

AI

Artificial Intelligence

Software that can perform tasks normally associated with human intelligence.

ESSENTIAL

API Key

Application Programming Interface Key

A secret code that lets software access an online service.

USEFUL

BYOK

Bring Your Own Key

A setup where the user supplies their own API key instead of the provider holding it.

USEFUL

GPT

Generative Pre-trained Transformer

A type of AI language model used for text, chat and content generation.

USEFUL

GPU

Graphics Processing Unit

A chip used for graphics and heavy AI processing.

USEFUL

Hallucination

AI Hallucination

When AI produces something that sounds confident but is wrong or unsupported.

USEFUL

LLM

Large Language Model

An AI model trained to understand and generate text.

USEFUL

ML

Machine Learning

A type of AI where systems learn patterns from data.

USEFUL

NLP

Natural Language Processing

Technology that helps computers understand human language.

USEFUL

NPU

Neural Processing Unit

A chip designed to run AI tasks efficiently.

USEFUL

OCR

Optical Character Recognition

Technology that reads text from images, scans or photos.

USEFUL

Prompt

AI Instruction

The instruction or question given to an AI system.

USEFUL

RAG

Retrieval-Augmented Generation

AI that looks up information from documents or databases before answering.

USEFUL

STT

Speech-to-Text

Technology that turns speech into written text.

USEFUL

TTS

Text-to-Speech

Technology that turns written text into spoken audio.

CATEGORY

Hardware, Devices and Access

USEFUL

BYOD

Bring Your Own Device

Staff using personal devices for work.

USEFUL

COPE

Corporate-Owned, Personally Enabled

A company-owned device that staff can also use personally.

USEFUL

CPU

Central Processing Unit

The main processor in a computer.

USEFUL

CYOD

Choose Your Own Device

Staff choosing from approved company devices.

USEFUL

HDD

Hard Disk Drive

Older-style spinning disk storage.

USEFUL

HDMI

High-Definition Multimedia Interface

A connection for video and audio to screens.

USEFUL

MDM

Mobile Device Management

Software used to manage company phones, tablets and laptops.

USEFUL

NFC

Near Field Communication

Short-range wireless communication, often used for contactless payments.

USEFUL

QR Code

Quick Response Code

A square barcode scanned by a phone.

USEFUL

RAM

Random Access Memory

Short-term working memory used while a device is running.

USEFUL

SSD

Solid State Drive

Fast storage used in modern computers.

USEFUL

UEM

Unified Endpoint Management

Managing many types of devices from one system.

USEFUL

USB

Universal Serial Bus

A common connection for devices, charging and data.

USEFUL

USB-C

Universal Serial Bus Type-C

A modern reversible USB connector.

CATEGORY

Finance, Payments and Online Trading

USEFUL

AML

Anti-Money Laundering

Rules and checks designed to prevent criminal money movement.

USEFUL

EPOS

Electronic Point of Sale

A digital till and sales system.

USEFUL

HMRC

His Majesty's Revenue and Customs

The UK tax authority.

USEFUL

KYC

Know Your Customer

Checks used to confirm a customer's identity.

USEFUL

MTD

Making Tax Digital

UK tax rules requiring digital records and submissions for some businesses.

USEFUL

PCI

Payment Card Industry

The card payment security ecosystem.

SECTOR-SPECIFIC

PCI DSS

Payment Card Industry Data Security Standard

Security rules for handling payment card data.

USEFUL

POS

Point of Sale

The system where a customer pays.

USEFUL

PSP

Payment Service Provider

A company that processes payments, such as card or online payments.

USEFUL

VAT

Value Added Tax

A tax added to many goods and services.

Procurement, Public Sector and NHS-Related Terms

SECTOR-SPECIFIC

CCS

Crown Commercial Service

The UK government organisation that supports public sector procurement.

SECTOR-SPECIFIC

CNI

Critical National Infrastructure

Essential services and systems such as energy, water, transport and healthcare.

SECTOR-SPECIFIC

DPS

Dynamic Purchasing System

A public sector purchasing system suppliers can join if they qualify.

SECTOR-SPECIFIC

DSPT

Data Security and Protection Toolkit

An NHS information governance and security self-assessment tool.

SECTOR-SPECIFIC

G-Cloud

Government Cloud Framework

A UK public sector framework for buying cloud services.

SECTOR-SPECIFIC

ICB

Integrated Care Board

NHS organisation responsible for planning health services in a local area.

SECTOR-SPECIFIC

ICS

Integrated Care System

Local partnerships between NHS, councils and other organisations.

SECTOR-SPECIFIC

ITT

Invitation To Tender

A formal invitation to bid for work.

SECTOR-SPECIFIC

NHS

National Health Service

The UK public healthcare system.

SECTOR-SPECIFIC

PPN

Procurement Policy Note

Public sector procurement guidance.

SECTOR-SPECIFIC

RFP

Request For Proposal

A request asking suppliers to propose a solution and price.

SECTOR-SPECIFIC

RFQ

Request For Quotation

A request asking suppliers to provide pricing.

Quick Cards

DO I NEED
TO CARE?

Yes. This is one of the most important basic protections a business can use.

MFA / 2FA

Multi-Factor Authentication / Two-Factor Authentication

MFA means logging in with more than just a password. For example, you enter your password and then approve the login using an app, code, fingerprint or security key.

Why it matters

Passwords get stolen, guessed and reused. MFA helps stop criminals getting into accounts even if they know the password.

SME action

Turn MFA on for email, banking, Microsoft 365, Google Workspace, accounting software, website admin accounts, cloud storage and anything holding customer or payment information.

DO I
NEED TO
CARE?

Yes, especially if customers, insurers or public sector buyers ask about your cybersecurity.

CE / Cyber Essentials

Cyber Essentials

Cyber Essentials is a UK cybersecurity certification that checks whether your business has basic protections in place.

Why it matters

It helps show that your business takes cybersecurity seriously. It may also be requested when bidding for certain contracts or working in supply chains.

SME action

Check whether your business could pass the basic Cyber Essentials requirements. Focus on secure settings, updates, access control, malware protection and firewall protection.

DO I NEED TO
CARE?

Maybe. It depends who you
sell to.

CE+ / Cyber Essentials Plus

Cyber Essentials Plus

Cyber Essentials Plus is the stronger version of Cyber Essentials because it includes independent technical testing.

Why it matters

Some customers may trust Cyber Essentials Plus more because it is not just a self-assessment.

SME action

Start with Cyber Essentials first. Consider Cyber Essentials Plus if you work with larger clients, public sector buyers, sensitive data or regulated industries.

DO I NEED TO
CARE?

Yes, if your business handles
personal data.

GDPR / UK GDPR

General Data Protection Regulation / United Kingdom GDPR

UK GDPR is the law covering how organisations collect, store, use, share and protect personal information.

Why it matters

Customer names, email addresses, phone numbers, addresses, employee records, order histories and marketing lists can all count as personal data.

SME action

Know what personal data you hold, why you hold it, where it is stored, who can access it and how long you keep it.

DO I NEED TO
CARE?

Yes, if your business handles
personal data.

ICO

Information Commissioner's Office

The ICO is the UK regulator for data protection and information rights.

Why it matters

The ICO provides guidance for businesses and can deal with complaints or data protection issues.

SME action

Use ICO guidance when writing privacy notices, handling customer data, managing cookies or dealing with data requests.

DO I NEED TO CARE?

Sometimes.

DPIA

Data Protection Impact Assessment

A DPIA is a risk assessment for privacy. It helps you think through whether a project could create risks for people's personal data.

Why it matters

A DPIA may be needed when using sensitive data, monitoring people, introducing new technology or doing something that could affect privacy.

SME action

Carry out a DPIA before launching systems that involve sensitive personal data, tracking, surveillance, profiling or unusual use of customer information.

DO I NEED
TO CARE?

Yes, if you store personal data about customers, staff or users.

SAR / DSAR

Subject Access Request / Data Subject Access Request

A SAR is when someone asks to see what personal data your business holds about them.

Why it matters

Businesses need to know how to recognise and respond to these requests properly.

SME action

Have a simple internal process for handling personal data requests. Make sure staff know who to pass them to.

DO I NEED
TO CARE?

Yes, if you rely on email for customers, invoices, bookings or marketing.

DKIM

DomainKeys Identified Mail

DKIM adds a digital signature to outgoing email so receiving systems can check that the message has not been tampered with.

Why it matters

It helps prove that your email is legitimate.

SME action

Make sure DKIM is enabled in Microsoft 365, Google Workspace, Mailchimp, Shopify or whatever platform sends email on your behalf.

DO I NEED
TO CARE?

Yes, if your business sends email from its own domain.

SPF

Sender Policy Framework

SPF is a domain setting that says which mail servers are allowed to send email for your business.

Why it matters

It helps reduce fake emails pretending to come from your domain.

SME action

Ask your domain, website or IT provider whether SPF is correctly set up for your business email.

DO I NEED
TO CARE?

Yes. This is becoming increasingly important for business email trust.

DMARC

Domain-based Message Authentication, Reporting and Conformance

DMARC tells receiving mail systems what to do when an email fails SPF or DKIM checks.

Why it matters

It helps stop criminals spoofing your domain and pretending to be your business.

SME action

Set up DMARC carefully. Start with monitoring, then move towards stricter protection once legitimate email sources are confirmed.

DO I NEED
TO CARE?

**Yes, especially if your business has
laptops, desktops or servers.**

EDR

Endpoint Detection and Response

EDR watches devices for suspicious activity and helps detect attacks that basic antivirus may miss.

Why it matters

Modern attacks do not always look like traditional viruses. EDR can spot unusual behaviour, such as strange scripts, stolen credentials or attacker movement.

SME action

Ask your IT provider what protection is installed on business devices. Do not assume basic antivirus is enough for every situation.

DO I NEED TO
CARE?

**Yes, but do not treat it as a
magic shield.**

VPN

Virtual Private Network

A VPN creates a secure connection between a device and another network or service.

Why it matters

VPNs are often used for remote access to business systems. Poorly configured VPNs can also become a target.

SME action

Use VPNs only where needed, keep them updated, protect them with MFA and remove access for people who no longer need it.

DO I NEED
TO CARE?

**Yes. Every business should have at
least a simple version.**

BCP

Business Continuity Plan

A BCP explains how the business keeps going during disruption.

Why it matters

Cyberattacks, power cuts, internet outages, supplier failures and lost devices can all stop work.

SME action

Write down what happens if email, payments, website, phones, files or key software are unavailable.

DO I NEED TO CARE?

Yes.

DR

Disaster Recovery

Disaster recovery is how you restore systems, files and data after a serious failure.

Why it matters

Backups are only useful if they can actually be restored.

SME action

Check that backups exist, are recent, are protected from ransomware and have been tested.

DO I NEED TO CARE?

Yes, if downtime costs your business money.

RTO

Recovery Time Objective

RTO means how quickly you need a system back after it fails.

Why it matters

Some systems can be down for a day. Others need to be restored within an hour.

SME action

Decide which systems are critical and how long the business can survive without each one.

DO I NEED TO CARE?

Yes, if losing data would hurt the business.

RPO

Recovery Point Objective

RPO means how much data you can afford to lose.

Why it matters

If your backup runs once per day, you may lose up to a day's work.

SME action

For critical systems, make sure backup frequency matches the amount of data loss the business can tolerate.

DO I NEED TO CARE?

Yes, if you outsource IT.

MSP

Managed Service Provider

An MSP is an external company that manages IT support, devices, updates, users, networks and systems.

Why it matters

Many SMEs rely on MSPs, but not all MSPs provide the same level of security.

SME action

Ask exactly what is included: updates, backups, MFA, device protection, monitoring, documentation and incident support.

DO I NEED TO CARE?

Maybe.

MSSP

Managed Security Service Provider

An MSSP is a provider focused specifically on cybersecurity services.

Why it matters

An MSP may handle general IT, while an MSSP may provide monitoring, response, vulnerability management and security advice.

SME action

Consider MSSP support if your business handles sensitive data, has compliance obligations or cannot monitor security internally.

DO I
NEED TO
CARE?

Yes, if your business uses AI tools, integrations, payment systems or connected software.

API Key

Application Programming Interface Key

An API key is a secret code that lets one piece of software access another service.

Why it matters

If an API key is leaked, someone else may be able to use your account, access data or create charges.

SME action

Treat API keys like passwords. Do not paste them into public websites, screenshots, documents or support chats.

DO I NEED TO
CARE?

Yes, if using AI or cloud-connected tools.

BYOK

Bring Your Own Key

BYOK means the user supplies their own API key instead of the software provider holding or reselling access.

Why it matters

It can give the customer more control, but it also means the customer must manage the key safely.

SME action

Use separate keys for separate tools where possible. Revoke keys that are no longer needed.

DO I NEED
TO CARE?

Yes, especially for reputation, security and fraud prevention.

OSINT

Open Source Intelligence

OSINT means information gathered from public sources such as websites, company records, search engines, social media and public documents.

Why it matters

Attackers, scammers and competitors can use public information about your business. You should know what is visible.

SME action

Search for your business, directors, email addresses, old documents, exposed files and outdated public information.

DO I
NEED TO
CARE?

Maybe. Most small businesses do not need to run one themselves, but they should understand the term.

SIEM

Security Information and Event Management

A SIEM collects logs from systems and helps identify suspicious activity.

Why it matters

It can help detect attacks, but it needs proper setup and monitoring.

SME action

If a provider mentions SIEM, ask who monitors it, what alerts are reviewed and what happens when something serious is found.

DO I NEED TO
CARE?

Maybe, depending on business
size and risk.

SOC

Security Operations Centre

A SOC is a team that monitors security alerts and responds to cyber incidents.

Why it matters

Security tools are only useful if someone pays attention to the alerts.

SME action

Ask whether your provider offers real monitoring or simply installs tools and leaves them running.

DO I
NEED TO
CARE?

Usually only if your business works in
regulated, essential or important
services.

NIS

Network and Information Systems

NIS rules focus on the cyber resilience of important services and digital infrastructure.

Why it matters

Some organisations have specific legal duties because the services they provide are important to society or the economy.

SME action

If you supply public sector, healthcare, energy, transport, digital infrastructure or other critical sectors, check whether your customers expect NIS-related controls from suppliers.

DO I
NEED TO
CARE?

Potentially, especially if your business
supplies regulated sectors or critical
services.

CSR Bill

Cyber Security and Resilience Bill

This is UK legislation intended to update cyber resilience rules and strengthen protection for important services.

Why it matters

Even where SMEs are not directly regulated, larger customers may pass cyber requirements down through contracts and supplier checks.

SME action

Watch for supplier security requirements from customers in healthcare, public sector, digital services and critical infrastructure.

Simple SME Priority List

1. Turn on MFA for important accounts.
2. Use a password manager and stop reusing passwords.
3. Keep devices and software updated.
4. Protect business email with SPF, DKIM and DMARC.
5. Make sure backups exist and can be restored.
6. Know what personal data the business holds.
7. Keep admin access limited.
8. Remove old users and unused accounts.
9. Ask IT suppliers what they actually monitor.
10. Consider Cyber Essentials as a practical baseline.

USE AND SOURCES

Free to download. Still Aldermere copyright.

This free giveaway may be downloaded and shared as an unmodified Aldermere Systems resource. It may not be resold, rebranded, or presented as another organisation's work.

Checked against public guidance from NCSC, ICO, IASME and GOV.UK at time of publication. Guidance and scheme wording can change, so use current official sources for formal decisions.

Copyright (c) 2026 Aldermere Systems. All rights reserved.