

POWERED BY  Microsoft 365

## Protect the vital business data that you hold in SharePoint, Teams and OneDrive with scanning against malicious files using Advanced Threat Protection (ATP)

Microsoft 365 brings together Office 365, Windows 10, and Enterprise Mobility + Security (EMS) thus empowering everyone to be creative and work together, securely.

Once you have correct the licence in place though, the security and compliance functionality in EMS needs to be enabled.

At Grant McGregor we don't believe in complicating things with bespoke scoping exercises and drawn-out implementation. That's why we've created our one-off, fixed price, fixed-scope M365 Security & Compliance Packs which unlock the tailored functionality needed to help protect your business appropriately.

Advanced Threat Protection (ATP) Pack enables seamless security features which protect end-users from accidentally sharing data or from being targeted by a phishing attack.

Book a 15-minute chat  
to get more info  
<https://grmc.it/atp>

**Advanced Threat Protection for all your users and vital business data**

**now included in  
Business Premium**



Enabled for SharePoint, Teams and OneDrive, ATP scans files stored with these services to help keep your business safe.

### Advanced Threat Protection enables:

- 1 Safe Attachments
- 2 Safe Links
- 3 Personal User Quarantine
- 4 Identification and Blocking of Malicious Files
- 5 Anti-Phishing and SPF Protection
- 6 Online Exchange Archiving
- 7 Prevention of Forwarding to External Domains

POWERED BY  Microsoft 365

## Ensure secure passwords, enable Multi Factor Authentication (MFA) and give your people the ability to reset their own passwords



**M365 Security & Compliance Packs** which unlock the tailored functionality needed to help protect your business appropriately.

Book a  
15-minute chat  
to get more info

<https://grmc.it/cim>

Enable vital password security, user access authentication and self-service password resets

now included in  
**Business Premium**

Microsoft 365 brings together Office 365, Windows 10, and Enterprise Mobility + Security (EMS) thus empowering everyone to be creative and work together, securely.

Once you have the correct licence in place though, the security and compliance functionality in EMS needs to be enabled.

At Grant McGregor we don't believe in complicating things with bespoke scoping exercises and drawn-out implementation.

That's why we've created our one-off, fixed price, fixed-scope M365 Security & Compliance Packs which unlock the tailored functionality needed to help protect your business appropriately.

### Cloud Identity Management enables:

- 1 Synchronised Identities with On-Premise AD
- 2 Secure Password Policies & Passwordless Sign-in
- 3 Self-Service Password Reset
- 4 Conditional Access MFA with Safe Zones
- 5 Conditional Access MFA for Guest Accounts
- 6 Corporate Branding
- 7 Windows Hello policies

POWERED BY  Microsoft 365

## Classify and protect data and files in your organisation - ensuring only data that should, can leave your business network.

Microsoft 365 brings together Office 365, Windows 10, and Enterprise Mobility + Security (EMS) thus empowering everyone to be more creative and work together, securely.

Once you have the correct licence in place though, the security and compliance functionality in EMS needs to be enabled.

At Grant McGregor we don't believe in complicating things with bespoke scoping exercises and drawn-out implementation.

That's why we've created our one-off, fixed price, fixed-scope M365 Security & Compliance Packs which unlock the tailored functionality needed to help protect your business appropriately.

Cloud Information Protection allows document classification in line with pre-configured labels, such as Private or Confidential. These labels live with the document and can be used to prevent things like printing, downloading, emailing of a document.



An on-premises scanner helps further identify files that may need to be labelled.

**Classify documents in-app or using right-click functionality. Our implementation service enables additional file types to be classified.**

Book a 15-minute chat  
to get more info  
<https://grmc.it/cip>

**Protect your business data with simple to use classification, policies and labelling**

**now included in Business Premium**

### Cloud Information Protection enables:

- 1** Creation of five GrMc Data labels to categorise data sensitivity
- 2** Five Data policies to determine how sensitive data is handled
- 3** Prevention of sensitive data leaving your business network
- 4** Deployment support for Azure Information Protection Client
- 5** Reporting and alerting

POWERED BY  Microsoft 365

**Identify sensitive information that lives on your business network.  
Then keep it safe - by ensuring it only leaves the network when  
given appropriate permission.**



**Our Data Loss Prevention Pack can help you identify Personally Identifiable Information (PII) as well as sensitive business data across your Microsoft applications. Once identified you can track where and how this data can be stored and transmitted.**

Book a 15-minute chat  
to get more info

<https://grmc.it/dlp>

**Protect personal information and  
comply with GDPR regulations**

**now included in  
Business Premium**

Microsoft 365 brings together Office 365, Windows 10, and Enterprise Mobility + Security (EMS) thus empowering everyone to be more creative and work together, securely.





Once you have the correct licence in place though, the security and compliance functionality in EMS needs to be enabled.

At Grant McGregor we don't believe in complicating things with bespoke scoping exercises and drawn-out implementation.

That's why we've created our one-off, fixed price, fixed-scope M365 Security & Compliance Packs which unlock the tailored functionality needed to help protect your business appropriately.

Data Loss Prevention allows the configuration of expressions (such as credit card number), these can be a specific set of numbers and letters, or a format that this information would typically appear in. Such data can then be blocked from leaving the business, or simply reported on to your in-house data management officer or team.

## Data Loss Prevention Key Points:

-  Define sensitive GDPR and Financial data policies across Email, SharePoint and OneDrive
-  Prevent Personally Identifiable Information being sent outside of the organisation using MS GDPR and Financial Policies
-  Streamline GDPR Compliance using MS GDPR DLP
-  Configure DLP reports and alerting

POWERED BY  Microsoft 365

**Ensure that only permitted devices and applications that are properly setup can access your Microsoft 365 (MS365) data.**



Employees are bringing their own devices and accessing your corporate data on them. Our Device Security Pack helps secure your business information from threats and leaks.

Book a 15-minute chat to get more info

<https://grmc.it/dm>

Enable basic device security to maintain the integrity of your data and your business network

now included in Business Premium







Microsoft 365 brings together Office 365, Windows 10, and Enterprise Mobility + Security (EMS) thus empowering everyone to be more creative and work together, securely.

Once you have the correct licence in place though, the security and compliance functionality in EMS needs to be enabled.

At Grant McGregor we don't believe in complicating things with bespoke scoping exercises and drawn-out implementation. That's why we've created our one-off, fixed price, fixed-scope M365 Security & Compliance Packs which unlock the tailored functionality needed to help protect your business appropriately.

Apply data policies on both corporate and employee devices alike, to safeguard your business data. In the event that a device is lost or stolen, this pack means you can then remotely wipe business data.

### Device Security enables:

-  GM Protection Policy and Configuration (Enrolment of Device and encryption of corporate data)
-  Enforcement of MFA to access Outlook app
-  Prevention of unofficial apps to connect to MS365
-  Enable remote wipe of business data stored on device
-  Controlled folder access and attack surface reduction
-  Cyber Essentials Best Practice security baselines