Third Party Information Security Principles

Document Control

Title:	Third Party Information Security Principles
Owning Department:	Information Security
Version Number:	V1.3
Classification:	C1 - Public
Document Author:	Jack Hardacre
Document Owner	Peter Williams
EXCO Sponsor	Tricia Williams
Status	Approved
Reference	MAG-IS
Minimum Review Frequency	Annually
Next review Date	31 July 2019
Date Effective from	1 August 2018

Revision History

Version	Date	Changes	Other standards affected	Approved by
0.1	23/02/2018	First Draft	-	
0.2	07/06/2018	Second Draft	-	
1.0	28/08/2018	Final draft	None	Information Security Team
1.2	05/10/2018	Updated wording	N/A	Head of Cyber Risk & Compliance and Head of Cyber Engineering
1.3	17/04/2019	EXCO update		

Contents

1. Introduction

Manchester Airports Group (''MAG'') relies on the integrity and accuracy of its data in order to deliver its services to the highest standard. It is therefore paramount that the integrity, confidentiality and availability of MAG data is ensured. Any third party which processes or manages MAG information must adhere to these principles to ensure that MAG maintains the trust of all relevant stakeholders and remains in compliance with relevant legal and regulatory requirements.

1.1 Purpose

The purpose of this standard is to ensure that all third parties that are currently contracted with MAG will adhere to the minimum information security requirements expected of parties who have access to MAG information assets. This includes all third parties who are either data processors, or data controllers for MAG.

A formal contract between MAG and the third party must exist to protect both parties.

All contracts must be submitted to MAG Legal Services Department for accurate content, language and presentation.

This document sets out the minimum information security requirements expected of third parties who have access to MAG information during the provision of contracted services to MAG. The standard aims to effectively protect MAG information by providing a flexible yet consistent approach to managing information security risk in third party suppliers, and assist MAG suppliers to better understand and work co-operatively with MAG on proportionate security controls.

Outsourced employees, contractors and consultants working on behalf of MAG are subjected to background checks equivalent to those performed on permanent MAG employees.

Technical, administrative and physical access controls must be implemented for outsourced employees, contractors and consultants.

1.2 Scope

The scope of this standard includes any third party which will process or have access to MAG information. This includes, but is not limited to:

- Third parties involved in the design, development or operation of information systems for MAG e.g. writing and installing bespoke software, third party maintenance or operation of systems, outsourcing of facilities;
- Access to MAG information from remote locations where the computer and network facilities are not under the control of MAG;
- Users who are not employees of MAG and require access to MAG information or information systems;
- Software-As-A-Service (SaaS) providers that may process, store or have direct access (e.g. via VPN) to MAG data;
- Third parties that may offer data processing services to MAG using either their own or a remote Cloud platform, including in multi-tenant environments.

This standard therefore also applies to all staff, including contractors, temporary staff and third parties employed directly and indirectly by the Third Party organisation (e.g. subcontractors). If there is a direct conflict between any requirements of this standard and the terms of a written agreement between the supplier and MAG, the terms of the written contract will prevail to the extent of the conflict.

1.3 Ownership and Document Change Control

This standard is owned and maintained by the MAG Information Security Team and can be amended with or without notice from time to time at MAG's discretion. Third Parties will not be expected to comply with any changes to this document until they have been provided with such changes in writing and a reasonable period (not to exceed 120 days) to comply with such changes.

The standard will be comprehensively reviewed by MAG's Information Security Team and updated as necessary every year.

Any queries or feedback relating to implementation or compliance should be directed to the MAG Information Security Team at IS.Security@magairports.com.

1.4 Information Security Reviews

Third parties may be subject to compliance reviews against this Standard and will be required to comply with the requirements herein, where the controls are applicable, proportionate and appropriate.

Third parties must document any security elements and controls that have been implemented to comply with this Standard in order to assist with any information security reviews carried out by MAG or nominated parties.

1.5 Exceptions

MAG security standards are in place to assist MAG and its suppliers in complying with information security best practices, legislative and regulatory requirements. Where it is not feasible for the third party to comply with any of the specific control requirements defined in this Standard, approval will be required from the MAG Information Security Team. Each non-compliance will be evaluated and risk-assessed, and either the risk accepted by the MAG Information Security Team or the third party will be required to comply with the control and an implementation date agreed with the assistance of MAG’s Information Security Team. All waivers will be tracked in a register by the MAG Information Security Team and held by the Cyber Engineering function.

2. Information Security Policy

2.1 Information Security Policy

The Third Party shall at all times maintain a management-approved corporate Information Security Policy, or set of Information Security Policies, defining responsibilities and setting out the Third Party's approach to information security.

2.2 Industry Standards

The Third Party shall at all times maintain a supporting framework of policies covering all requirements set out in this document in line with industry best-practice, such as ISO 27001, ISO 27005 and PCI-DSS.

2.3 Publication and Communication

The Third Party shall at all times ensure that its Information Security Policies are published and effectively communicated to all staff responsible for MAG Information.

3 Third Party Organisation

3.1 Information Security Function

3.1.1 The third party shall designate named individuals or teams who will have responsibility and accountability for information security policy, implementation and processes. Such nominated individuals shall act as the primary points of contact for MAG where information security is concerned. Additionally, they shall facilitate any security review meetings and manage any restoration plan in the event of a security breach.

3.2 Processes and Procedures

3.2.1 Documented procedures must be in place to authorise significant changes to MAG Information processing procedures and to ensure relevant information security controls are maintained. All processes for managing the security of MAG Information must be assessed on a regular basis and communicated to the MAG Information Security Team.

3.2.2 The Third Party shall not process or otherwise make use of or share MAG information, for any purpose other than that which is directly required for the supply of the agreed Services.

3.2.3 The Third Party shall only perform such Services in accordance with the Contract.

3.2.4 The Third Party shall not purport to sell, let for hire, assign rights in or otherwise dispose of any of MAG information without the prior written approval of MAG.

3.2.5 The Third Party shall not commercially exploit MAG information or MAG Materials without the prior written approval of MAG.

3.2.6 The Third Party shall establish and at all times maintain safeguards against the accidental or deliberate or unauthorised disclosure, access, manipulation, alteration and against any destruction, corruption of, damage, loss or misuse of MAG information in the possession of the Third Party or any sub-contractors or agents of the Third Party.

3.3 Information Risk

3.3.1 The Third Party shall maintain a register of the security risks related to the provision of its Services to MAG and to MAG information. The risk register shall be maintained to show the nature and extent of, and progress made in, mitigating the identified risks.

4. Human Resource Security

4.1 Prior To Employment

Roles and Responsibilities

4.1.1 The Third Party shall ensure that information security roles and responsibilities of all Third Party employees (and subcontractors) are clearly defined and documented.

4.1.2 The Third Party shall (and shall procure that its Subcontractors shall) have a comprehensive disciplinary policy, code of conduct & work rules directive in force to protect the interests and safety of Third Party and Subcontractor personnel and the Services, and the security of MAG personnel and information. That policy shall clearly define what breaches of security represent misconduct and what consequences shall be incurred.

Screening

4.1.3 The Third Party shall ensure that its personnel application and contractual process contain a series of declarations that the applicant must make to cover criminal convictions as per the terms of the Rehabilitation of Offenders Act 1974, pending criminal investigations or adverse financial probity judgements such as county court judgments or bankruptcy rulings.

4.1.4 If the declarations or the relevant Criminal Record Check, in relation to a Third Party or Subcontractor staff member, reveal any convictions then the Third Party shall in every case immediately bring this to MAG's attention for consultation. In such circumstances, MAG shall have the right to require that the relevant staff member is removed from participating in the provision of the Services.

4.1.5 Where the Third Party's business function includes financial payment transactions, the Third Party shall ensure that a financial probity check (covering adverse County Court Judgments and bankruptcy rulings) is conducted with Experian or other reputable agency (the "Financial Probity Check") against all Third Party and Subcontractor personnel involved in the provision of the Services. If the declarations or the relevant Financial Probity Check reveal any adverse County Court Judgments or bankruptcy rulings, then the Third Party shall immediately notify MAG for consultation. In such circumstances, MAG shall have the right to require that the relevant staff member is removed from participating in the provision of the Services.

4.1.6 The Third Party shall ensure that all above-mentioned background checks ("Background Checks") shall be conducted at the Third Party's cost and within a reasonable time period and in any event shall be completed prior to such Third Party or Subcontractor personnel commencing provision of the Services (excluding training). The Third Party shall bear all training and attrition costs if any Third Party or Subcontractor personnel are removed from the Services because of a positive disclosure on any declaration or Background Check.

Employment References

4.1.7 The Third Party shall ensure that a written policy exists and is followed for pre-employment screening and that the screening status and results for all Third Party personnel are fully collated, kept on record and made available to MAG on MAG's written request for audit and compliance purposes

4.1.8 The Third Party shall obtain two references prior to its personnel completing training and commencing work. Such references may be verbal, but must be verified, fully documented and auditable. Where reasonably possible, the Third Party shall obtain at least one such reference from a previous employer or academic professional.

Contractual Agreements

4.1.9 The Third Party shall ensure that all personnel enter into a written contract of employment under which they agree to adhere to all Third Party policies, rules and procedures including all information protection policies and agree to assign all intellectual property created in the course of providing the Services to the Third Party so that the intellectual property provisions of the Contract can take effect.

4.1.10 The Third Party shall ensure that all personnel working in the provision of the Services sign an appropriate employee non-disclosure agreement relating to MAG information in the possession of the Third Party before they are given access to any such MAG Information.

4.2 During Employment

New Employee Induction

4.2.1 The Third Party shall ensure that a Security module forms part of the compulsory induction and training programme for all Third Party personnel involved in the provision of the Services. Such security module shall be sufficient to include information protection and security, the password and user account policy, issues of confidentiality and company security standards.

4.2.2 The Security Module shall as a minimum:

- Define the meaning and importance of information security;
- Underline the importance of complying with relevant information security policies and procedures and applying information security practices when processing MAG Information;
- Outline employee and Third Party responsibilities for the protection MAG Information including reporting suspected and actual information security incidents with regards to MAG Information; and
- Make clear the consequences and disciplinary procedures for not complying with this policy.

Compliance with Policy

4.2.3 The Third Party shall ensure that all employees and Third Parties have read, understood and remain in compliance with applicable third party security policies and procedures.

Training and Awareness

4.2.4 The Third Party shall hold structured briefings with respect to security awareness and knowledge of fraud and security issues (focusing on the risks resulting from poor information security, and legal and regulatory requirements to protect information) with Third Party personnel and its Subcontractors throughout the provision of the Services and shall review such briefing requirements on a regular basis.

4.2.5 The Third Party shall ensure that all Third Party personnel (including Subcontractor personnel) have the appropriate skills and training to support the Services, and that all IT or Information Security personnel (including Subcontractor personnel) have been given the authority and training to appropriately discharge their responsibilities.

Disciplinary Procedure

4.2.6 Formal disciplinary procedures must be in place for employees and Subcontractors who breach any applicable security policy related to the protection of MAG information.

4.2.7 The Third Party shall consult MAG's Information Security Team where any of its personnel (or any Subcontractor personnel) are subject to a change of circumstance and are then assessed to be a risk to the Services or MAG Information.

4.3 Termination of Employment

4.3.1 The Third Party shall implement a JML (Joiners-Movers-Leavers) process, including a 'checklist' of actions, including exit interview where appropriate, prior to the conclusion of the departing personnel's employment and shall ensure that any Subcontractor shall do the same. This checklist of actions shall include cancellation of access control privileges and user IDs/passwords required for access to the Third Party (and/or Subcontractor) and MAG Systems and recovery of any asset(s) that may contain information relating to MAG and/or MAG Associated Company and all property of same (including but not limited to desktops, laptops, external storage media (USB sticks and external hard drives) mobile devices, such as mobile phones and tablets, books, correspondence, files, statistics, papers, reports, minutes, plans, records, surveys, diagrams, computer print-outs, computer disks, CDs, audio tapes, manuals, customer documentation or any other medium for storing information in whatever form), and any swipe cards or ID passes giving the departing personnel access to Third Party (and/or Subcontractor) or MAG premises or storage or both; and deletion of data relating in any way to MAG and/or MAG Associated Company stored on any asset or system which is not a MAG or MAG Associated Company system.

5. Third Party Chain Management

Authorised Access

5.1.1 The Third Party shall provide full details of any Subcontractor(s) that it intends to use in the provision of the Services; such details to include as a minimum company name, address, location, and type of Services to be provided and the volume, frequency and nature of MAG information to be used.

5.1.2 The Third Party shall not make MAG information available to any Subcontractor without the prior written approval of MAG.

Risk Assessed Access

5.1.3 The third party must carry out an information security risk assessment prior to any Third Party access and the results of this must also be submitted to the MAG Information Security Team.

5.1.4 The Third Party shall ensure that a SoD (Segregation of Duties) model is in place so that it is not reliant on any key single individual to support Services anywhere in its supply chain.

Controlled Access

5.1.5 The Third Party shall ensure that all Subcontractor agreements contain security controls, service definitions, service requirements and delivery levels commensurate with the requirements set out in this document, and that such are implemented, operated, and maintained by all Subcontractors at all times.

Compliance

5.1.6 The Third Party shall conduct annual security reviews of the Subcontractors where those Subcontractors have access to MAG information, and maintain detailed, written evidence of these audits to include any security risks, recommendations and remedial actions.

5.1.7 Third Party security reviews shall be conducted in accordance with the requirements set out in this document.

Contractual Agreements

5.1.8 Third Party Subcontractors must operate in accordance with non-disclosure clauses stipulated in agreements between the Third Party and the Subcontractor.

Contract Termination

5.1.9 Exit procedures and requirements must be included in any agreement between the Third Party and the Subcontractor and all Third Party access to MAG information must be revoked when no longer required.

6. Asset Management

6.1 Information Classification and Handling

MAG holds many information assets that must be protected against unauthorised access, disclosure, modification, or other misuse. Efficient management of these assets is also necessary to comply with legal obligations under the UK Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation (GDPR).

Different types of information assets require different security measures. Good classification is vital to ensuring effective information security and management. Each security classification listed in the summary tables within this standard has defined information management controls which determine how information assets should be handled throughout their lifecycle. These controls should be applied to all information assets held by Third Parties.

There are four classifications of information as follows:

Level	Classification	Definition
C1	Public	May be viewed by anyone, anywhere in the world.
C2	Internal	Access is available to all MAG colleagues.
C3	Confidential	Access is limited to specified MAG colleagues with appropriate authorisation or on a need to know basis.
C4	Highly Confidential	Access is controlled and restricted to a small number of named individuals /authorities.

Where possible, information should be marked or labelled with its relevant sensitivity level per MAG or the Third Party classification model, so that users who handle documents can be aware of the sensitivity of the information as well as handling procedures.

All information classified as ‘Confidential’ and ‘High Confidential’ shall be clearly marked.

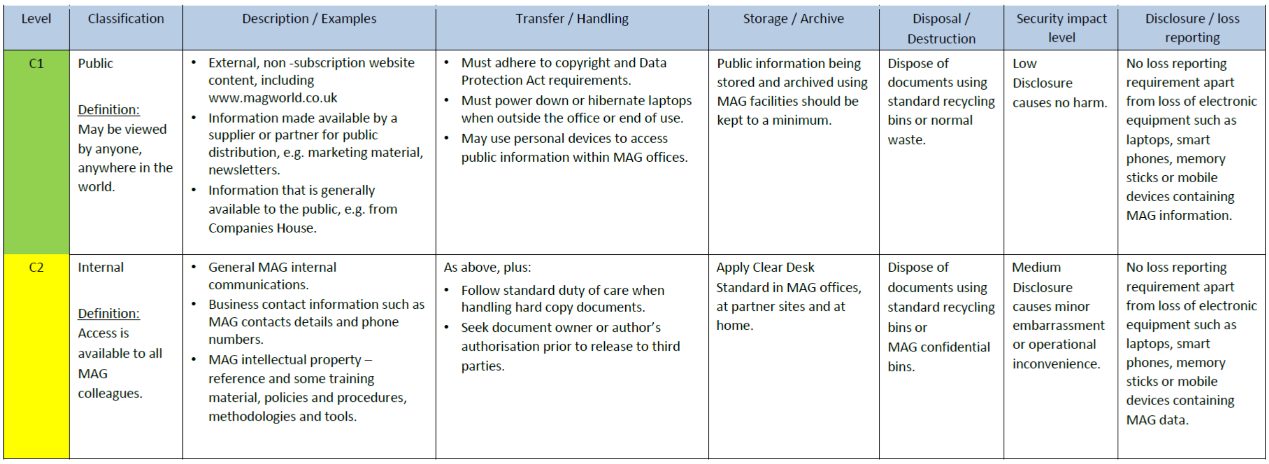
Documents such as those created with Microsoft Word, Excel, PowerPoint, or Visio should have the words “C3 - Confidential”, or “C4 – Highly confidential” clearly visible on each page where applicable.

6.1.1 The Third Party shall ensure that MAG Information is classified in terms of its value, legal requirements, sensitivity and criticality.

6.1.2 The Third Party shall ensure that an appropriate set of procedures for information labelling and handling is developed and implemented in accordance with the classification scheme adopted by the Third Party, and that such procedures are reviewed as a result of any significant business changes.

6.2 Handling and Classification Guidelines

6.2.1 The following table details the controls that shall put in place according to how the information is handled, e.g. transfer, storage and archive, disposal/destruction, and the requirement for reporting loss for each classification. These are set out cumulatively, whereby the set of controls for each classification builds upon the preceding level.



Level	Classification	Description / Examples	Transfer / Handling	Storage / Archive	Disposal / Destruction	Security impact level	Disclosure / loss reporting
C1	Public Definition: May be viewed by anyone, anywhere in the world.	• External, non -subscription website content, including www.magworld.co.uk • Information made available by a supplier or partner for public distribution, e.g. marketing material, newsletters. • Information that is generally available to the public, e.g. from Companies House.	• Must adhere to copyright and Data Protection Act requirements. • Must power down or hibernate laptops when outside the office or end of use. • May use personal devices to access public information within MAG offices.	Public information being stored and archived using MAG facilities should be kept to a minimum.	Dispose of documents using standard recycling bins or normal waste.	Low Disclosure causes no harm.	No loss reporting requirement apart from loss of electronic equipment such as laptops, smart phones, memory sticks or mobile devices containing MAG information.
C2	Internal Definition: Access is available to all MAG colleagues.	• General MAG internal communications. • Business contact information such as MAG contacts details and phone numbers. • MAG intellectual property – reference and some training material, policies and procedures, methodologies and tools.	As above, plus: • Follow standard duty of care when handling hard copy documents. • Seek document owner or author's authorisation prior to release to third parties.	Apply Clear Desk Standard in MAG offices, at partner sites and at home.	Dispose of documents using standard recycling bins or MAG confidential bins.	Medium Disclosure causes minor embarrassment or operational inconvenience.	No loss reporting requirement apart from loss of electronic equipment such as laptops, smart phones, memory sticks or mobile devices containing MAG data.

Level	Classification	Description / Examples	Transfer / Handling	Storage / Archive	Disposal / Destruction	Security impact level	Disclosure / loss reporting
C3	Confidential Definition: Access is limited to specified MAG colleagues with appropriate authorisation or on a need to know basis.	• Commercially confidential information, where not Highly Confidential, however held by us. • Internal MAG communications and information with a restricted audience. • General vendor accounts payable information, list of debtors, information held on the financial systems or extracted from and/or held on other systems. • Personal data related to customers, Board members, staff or other individuals, e.g. personnel records, home address, personal phone numbers, salary and bonus information. • Personal data in CRMs that is more detailed than business card data.	As above, plus: • Should clearly mark all MAG reports, spreadsheets, PowerPoints and PDF documents as 'Confidential' in document header/footer. • Restrict access to a 'need to know' basis. • Exercise diligence when taking hardcopy documents outside MAG offices. • Avoid taking from MAG site wherever possible. • Must only take hardcopy documents from office if transferred directly to/from office to destination (not via the pub, gym, etc). • Consider using secure post/courier. • Use MAG encrypted USB drives (memory sticks) or WinZip encrypted files for CDs and DVDs. • When sending email external to MAG, must encrypt attachments using WinZip (select 256 bit) or an equivalent encryption method (minimum 256 bit) – use a strong password exchanged by a different method, e.g. by text or phone. • C3 information must be encrypted using using WinZip (select 256 bit) or an equivalent encryption method (minimum 256 bit) – use a strong password exchanged by a different method for information at rest and in transit.	As above, plus: • Must store hardcopy documents in locked premises when off site, e.g. home or hotel room safe, or use central file stores when at MAG sites. • Hold electronic personal data in approved applications (avoid saving to local drives). • Restrict access to 'need to know' and review access rights periodically.	Dispose of documents using MAG confidential bins or a high quality, crosscutting shredder if not in a MAG office. Follow MAG Records Retention and Disposal Standard.	High Disclosure has a significant short term impact on operations and/or tactical objectives.	Must be reported immediately to the Chief Information Security Officer.
C4	Highly Confidential Definition: Access is controlled and restricted to a small number of named individuals /authorities.	• Highly confidential commercial information however held by us (i.e. whether as provided to us by the client/3rd party, within MAG generated reports, correspondence or other documents, or held on MAG IT systems or portable devices) including: – Price sensitive or otherwise material information, e.g. related to unannounced results, valuations, merger and acquisition related information. – Highly sensitive intellectual property e.g. for cutting edge technology or high profile designs and inventions. – Any other information deemed by MAG or partners to be highly sensitive, e.g. major restructurings, redundancies etc. • Personal data classed as 'sensitive' under the Data Protection Act 1998, e.g. political/religious views, sexual orientation, health. • Credit card and other payment card data. In general, data will be Highly Confidential if loss would result in a VERY difficult conversation with our customers and business partners.	• Should clearly mark all MAG reports, spreadsheets, PowerPoints and PDF documents as 'Highly Confidential' in document header/footer. • Must not use portable media as permanent storage. • Copy to MAG IT network any files created on smartphones or tablets. • When sending email external to MAG, must encrypt attachments using WinZip (select 256 bit) or an equivalent encryption method (minimum 256 bit) – use a strong password exchanged by a different method, e.g. by text or phone. • Where possible, seek to anonymise/cleanse data prior to collection or transfer – only collect or transfer what is needed. • C4 information must be encrypted using using WinZip (select 256 bit) or an equivalent encryption method (minimum 256 bit) – use a strong password exchanged by a different method for information at rest and in transit.	• Store hardcopy documents in locked rooms/ cabinets and/or central file stores. • Do not remove manual records from MAG sites unless absolutely necessary. If it is necessary, use safes for storage of documents and portable devices during overnight stays in hotels and never leave information in the boot of your car when you are not present etc. • Must not use portable media as permanent storage and must ensure deletion before and after use. • Must review and update access rights on a frequent basis. • Consider using secure project rooms for highly sensitive projects.	Dispose of documents using a high quality, crosscutting shredder. Follow MAG Records Retention and Disposal Standard. Apply higher level of standard if instructed by UK Government agencies or other interested parties.	Very High Disclosure has serious impact on long term strategic objectives of MAG and / or puts the survival of MAG at risk.	Must be reported immediately to the Chief Information Security Officer.

6.3 Asset Inventory

6.3.1 All information assets used to process MAG Information must be recorded in a maintained inventory. All Third Party Subcontractors must also maintain a similar inventory.

6.3.2 The Third Party shall ensure that any media used to record, store or process MAG Information as part of the Services, including (but not limited to) hard copy output, laptops, USB sticks, pen drives, CDs, external hard drives or other magnetic media are securely handled, transported and encrypted and that their use is authorised.

6.4 Asset Ownership

6.4.1 All information assets used to process MAG Information must be owned by a designated officer of the Third Party organisation.

6.5 Acceptable Use Policy (AUP)

6.5.1 An AUP must be defined and communicated to all users processing MAG Information. The AUP must:

- define appropriate use of communications channels and devices used to process MAG Information;
- define appropriate use of the Internet, including prohibiting the transfer of MAG Information to personal email accounts or unauthorised cloud-based storage;
- include responsibilities relating to downloading, installing and use of unauthorised or illegal software or material to process MAG Information;
- make clear statements about consequences of non-compliance or breach of the AUP; and
- be communicated to the MAG Information Security Team.

7. Physical and Environmental Security

7.1 Policy

7.1.1 The Third Party shall (and shall ensure that its Subcontractors shall) implement a policy identifying the requirements for physical access and control of such access of its sites (or those of the Subcontractor from where Services are provided).

7.1.2 Without prejudice to any of MAG's remedies, sanctions against Third Party and Subcontractor staff for breaches of security requirements shall be governed by the Third Party's or the Subcontractor's disciplinary policy as appropriate.

7.2 Physical Security

7.2.1 The Third Party will not perform the Services from other locations without obtaining the prior written consent of MAG, and any relocation will be approved by and implemented at no additional cost to MAG (unless any relocation is due to a specific request from MAG) and without causing any material disruption to the business of MAG or MAG Services.

Site Changes

7.2.2 Significant changes to sites processing MAG Information must be approved by the MAG Information Security Team.

Shared Site

7.2.3 Where MAG agrees (either under the Contract or by prior written consent) to a shared Site, the Third Party shall as a minimum:

- segregate the area in which the Services are performed for MAG;
- implement a clearly defined area for performing the Services;
- ensure that the Services and facilities required to provide the Services to MAG are kept completely physically separate from the Third Party's other clients with dedicated exit/entrance points and clear divides as defined by partition walling or desk plans.

Secure Perimeter

7.2.4 The Third Party shall (and shall ensure that its Subcontractors shall) review the strength and effectiveness of the management of physical security controls at its Sites (or those of its Subcontractors from where the Services are provided) at least every six months.

7.2.5 Where an automated access control system is deployed at its Sites (or those of its Subcontractors from where the Services are provided), the Third Party shall (and shall ensure that its Subcontractors shall) ensure that the system logs all access control events, that this log is audited on an on-going basis and that it is integrated with a JML process.

7.2.6 In the event that such automated access control system is not able to check and verify all staff and contractors ID passes and/or prevent tailgating, the Third Party shall (and shall ensure that its Subcontractors shall) deploy a physical security function or other mitigating control to enforce compliance in this area.

7.2.7 The Third Party shall ensure that all Third Party personnel (and any Subcontractor personnel) are issued with unique ID passes from which they are individually identifiable and responsible, and which shall then be worn and visible at all times.

The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.8 The Third Party shall be responsible for retrieving the ID passes of any Third Party personnel (and any Subcontractor personnel) that have had their employment terminated, transferred or otherwise no longer require access to the Site(s). The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.9 The Third Party shall ensure that a robust policy is in force to manage loss of ID passes and ID passes left at home by Third Party personnel (and any Subcontractor personnel). The Third Party shall ensure that its Subcontractors will enforce a similar policy at any Subcontractor sites from where the Services are provided.

7.2.10 The Third Party shall operate a sign-in procedure for any visitors to the Sites, which, as a minimum, requires visitors to log their name, company, the time and date and the name of the person whom they are visiting at the relevant Sites. The Third Party shall ensure that its Subcontractors will operate a similar procedure at any Subcontractor sites from where the Services are provided.

7.2.11 The Third Party shall deny entry to visitors to the Sites who are not legitimately connected with the Services being performed unless they are duly authorised to do so by the appropriate Third Party management. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.12 The Third Party shall inform all visitors of the existence of Site security policies. The Third Party shall ensure that its Subcontractors will inform all visitors of the existence of site security policies at any Subcontractor sites from where the Services are provided.

7.2.13 The Third Party shall ensure that there is a manned guarding or other appropriate physical security presence on Sites which are processing or storing Sensitive MAG Information. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.14 The Third Party shall ensure that there is a physical security response capability during out of hours periods for those Sites storing or processing Sensitive MAG Information. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.15 The Third Party shall ensure security response personnel receive appropriate training in all security related policies. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.16 The Third Party shall ensure security response personnel are instructed to take action as appropriate or escalate the incident to a manager. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.17 The Third Party shall have in place an internal and external CCTV system with sufficient coverage to monitor reception areas, exit/entry points, and vulnerable or sensitive/confidential working areas. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.18 The Third Party shall implement, operate, support, and maintain alarm systems (including appropriate environmental alarms), and physical access mechanisms. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

8. Facilities and Equipment Security

The Third Party will comply with the requirements set out by MAG Health and Safety Standard and IT control of works process when accessing MAG facilities or handling equipment.

9. Communications and Operations Management

9.1 Operating Procedure Documentation

9.1.1 Operating procedures for information security management and controls related to MAG Information must be documented, maintained and made available to the relevant user involved in processing MAG Information.

9.2 Operational Separation of Duties

9.2.1 Duties and areas of responsibility must be segregated to reduce opportunities for unintentional or unauthorised modification or misuse of MAG Information.

9.2.2 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that development, testing, production and operational facilities are separated to reduce the risks of unauthorised access or changes to the operational system.

9.3 Malware Protection

Malware Incident Response

9.3.1 The Third Party shall promptly notify MAG in writing as soon as it becomes aware of any viruses in any Third Party Systems or MAG Systems, directly (or indirectly) affecting MAG Information, which have not been auto-corrected or detected and quarantined, and shall provide a written report to MAG describing the incident, the measures that were taken to resolve the incident and what measures were taken to prevent any reoccurrence.

Malware Protection Tool

9.3.2 The Third Party shall provide anti-virus protection software on all Third Party Systems vulnerable to virus infection and shall ensure that its Subcontractors shall do the same on any Subcontractor systems used in the provision of the Services in accordance with the requirements of this standard. The Third Party shall (and shall ensure that its Subcontractors shall) use all reasonable endeavours to detect hidden code or information that is designed to, or will have the effect of:

- destroying, altering, corrupting or facilitating the theft of any MAG Information; or
- disabling or locking any software or Third Party Systems or MAG Systems; or
- using undocumented or unauthorised access methods for gaining access to MAG Information, or Third Party or MAG Systems.

9.3.3 The Third Party shall ensure that anti-virus software and anti-virus definition files are updated for all Third Party Systems in line with best business practice and in accordance with advice from applicable anti-virus software. The Third Party shall also ensure that its Subcontractors shall do the same on any Subcontractor systems used in the provision of the Service.

9.3.4 The Third Party shall ensure that the malware protection tool deployed:

- is a current and supported version;
- is updated with definition or signature files on a daily basis as a minimum;
- provides real time on-access and on-demand scanning;
- scan all content entering and leaving the IT infrastructure processing MAG Information;
- is able to disinfect, quarantine or delete malware;
- can provide logging, alerts and reporting functionality; and
- cannot be disabled, reconfigured or prevented from working by unauthorised users.

9.3.5 The Third Party shall ensure that, where technically feasible, any device processing MAG Information must run the malware protection tool. This includes, but is not limited to, workstation, portable devices and servers. Where devices are technically unable to run the malware protection tool, then alternative mitigations shall be put in place to provide malware protection within the information processing chain.

9.4 Data Back-Up

9.4.1 The Third Party shall ensure that regular backups of all Third Party Systems hosting MAG information are performed, and their restoration tested, dependant on the frequency of information change.

9.4.2 The Third Party shall ensure that where Third Party Systems backups are stored off-site they are encrypted and securely transported, and a written register maintained of all backup tapes stored off-site.

9.4.3 The Third Party shall have processes in place ensure the recovery from the loss or damage of MAG Information or facilities used to process MAG Information.

9.4.4 The third party shall operate a back-up policy which mandates:

- the backing-up of MAG Information at scheduled risk-based intervals;
- validation of the back-ups;
- back-up retention periods;
- back-up type;
- media cycles and labelling; and
- a testing schedule.

9.4.5 The Third Party's back-up policy must be approved by the MAG Information Security Team.

9.5 Network Security Management

9.5.1 The Third Party shall (and shall ensure that its Subcontractors shall) maintain the appropriate confidentiality, integrity, and availability of MAG Information, by:

- Ensuring information is transmitted in encrypted form. The transport mechanism should use TLS 1.2 and higher. Data flow will be done by SFTP where practical.
- Internet traffic must go via Proxy servers.
- Production systems shall not use same environment as stage, testing, development or pre-production systems. Each environment must have a dedicated purpose.

- Ensuring when interfaces are exposed to non-trusted networks, they shall restrict access to specified and approved IP addresses. This can be achieved through access control lists or IP whitelisting.
- Third party direct access to systems is over encrypted VPN tunnel into a segregated network from where they will be granted access to central services in the required direction only
- All firewall rules are recorded and labelled according to use so that they can be removed after use
- No unsecured network ports will be placed in publicly accessible areas.
- Utilising secure network architecture and operations;
- Ensuring that networks carrying MAG Information are designed, built, monitored, and managed according to industry standards, best practices and frameworks e.g. ISO27001, TOGAF, OWASP ITIL, etc. such that they enforce the required information security policy boundaries. These boundaries must prevent unauthorised access to Systems and MAG Systems or MAG Information by default and allow only explicitly authorised and authenticated access.

9.5.2 Remote support access shall be controlled via a secure gateway that implements the following controls:

- strong authentication (e.g. two-factor authentication);
- access via a secure gateway (e.g. a firewall);
- remote support accounts only enabled for the duration of troubleshooting activity;
- all troubleshooting activity is logged and reviewed.

9.5.3 The Third Party shall seek prior written MAG approval to use any third party provider of remote support of Third Party systems. Any such approved Subcontractor shall be subject to a contract between the Third Party and such Subcontractor detailing security requirements in relation to such support, and that access granted to the Subcontractor in order to provide such support is given with minimum privileges and revoked on completion.

9.5.4 The Third Party shall develop and implement an appropriate internet, email and acceptable use policy and ensure that appropriate controls are in place and documented to prevent unauthorised download of software or web content by Third Party (or Subcontractor) personnel.

9.5.5 The Third Party shall ensure that utility programs capable of overriding system and application controls shall be restricted and tightly controlled.

9.5.6 The Third Party shall ensure that automatic equipment identification shall be used where appropriate as a means to authenticate connections from specific locations and equipment.

9.5.7 The Third Party shall have in place an intrusion detection strategy and upon request by MAG, provide written evidence as to what methods are employed, whether these are recognised intrusion detection systems or whether there is a reliance on other controls in place (firewalls, network router/switch protection) and whether the function is outsourced.

9.5.8 The Third Party shall ensure that regular penetration testing is carried out and shall agree in writing beforehand the scope of penetration testing for the Services with MAG. Further, the Third Party shall notify MAG in writing of the results of such testing and take action on the recommendations in timescales commensurate with the associated risks.

9.6 Platform and Application Security

9.6.1 The Third Party shall (and shall ensure that its Subcontractors shall) ensure:

- All web applications shall be developed in such a way as to be fully compliant with the latest version of 'The OWASP Guide to Building Secure Web Applications' as published by OWASP
- All processes that receive data input (both manual and automated) shall control and validate inputted data in terms of formatting, length and syntax.
- All web application code shall be statically tested, or penetration tested by an experienced penetration testing outfit.
- that standard platform builds are documented;
- all unnecessary services are removed from platforms or disabled, and remaining settings and software are security hardened;
- policies and procedures are developed and implemented to protect MAG Information associated with the interconnection of Third Party and MAG Systems; and
- all software installed on platforms is fully licensed and its use is authorised.

9.6.2 Where financial transactional functionality is (or becomes) a part of the Services, the Third Party shall provide information masking functionality in relation to software in respect of any financial information (including but not limited to debit/credit card and direct debit banking information) which Third Party (or its Subcontractors) handles for, or on behalf of, MAG.

9.7 System Management

9.7.1 The Third Party shall (and shall ensure that its Subcontractors shall) maintain Systems security measures to guard against the accidental, deliberate or unauthorised disclosure, access, manipulation, alteration, destruction, corruption of information through processing errors, damage or loss or misuse of MAG Information. As a minimum, these measures shall include software which:

- requires all users of the Systems to enter a username or identification number and password prior to gaining access to the Systems;
- controls and tracks the addition and deletion of users of Systems;
- controls, logs and tracks user access to areas and features of the Systems.

9.7.2 The Third Party shall provide MAG with a written record of such user access from time to time where MAG reasonably requests such information.

9.7.3 The Third Party shall update, monitor and review their systems regularly.

9.7.4 Where applicable, the Third Party shall ensure that Third Party System clocks are synchronised with an agreed accurate time source.

9.7.5 The Third Party shall ensure that sufficient physical and logical segregation is applied to any equipment operated by the Third Party for Services provided to MAG unless explicit written authorisation is given by MAG for exceptions.

9.7.6 The Third Party shall ensure that the Services are fully resilient unless MAG has confirmed in writing that this is not required.

9.7.7 The Third Party shall ensure that any faults are logged, investigated, prioritised and rectified in timescales commensurate with the associated risks.

9.7.8 The Third Party must have a Patching Policy and ensure that vendor patches are applied regularly. If there are exceptions to this, MAG must be informed.

9.8 Mobile Computing

9.8.1 The Third Party shall ensure that it adopts a policy to protect against the risk of using mobile computing and BYOD, teleworking activities and communication facilities where these are used to deliver Services to MAG.

9.9 Data Encryption

9.9.1 The Third Party shall transfer/exchange MAG Information via secure channels which are encrypted and further shall inform MAG in writing of the encryption solution used to transfer/exchange MAG Information in advance of any transfer or exchange. This solution must adhere to section 6 and is also applicable to MAG confidential data stored at off-site facilities.

9.9.2 All such transfer/exchange of MAG Information shall be compliant with all relevant agreements, laws, regulations and current industry best practice.

9.10 Monitoring and Audit Logs

9.10.1 Procedures must be in place to actively monitor for, review and act on any unauthorised processing of MAG Information.

9.10.2 Auditing of activities and information security events related to the processing of MAG Information must be kept in secure log files which are protected against unauthorised alteration or deletions and are backed-up in line with the back-up policy.

9.10.3 The logged information must include fields that are attributable to a single individual to ensure accountability and must be kept for an agreed time to assist with any possible investigations. Logs must be made available to the Information Security Team on request either as real-time or batch.

9.10.4 The system must produce, as a minimum, authentication and system configuration change logs. Log files created by the system must be made available to MAG for onboarding to the MAG SIEM tool. The log format should be available in open standards, eg. WMI or syslog.

10. Authentication and Access Control

The following sections set out the policy statements, principles and basic concepts that shall be adhered to by the third party for effective access control management within MAG.

10.1 Control Mechanisms

10.1.1 Access to MAG's information and information systems shall be controlled and permissions must be granted on a "need-to-know" basis and always following the "Least Privilege Principle". It is required that MAC (Mandatory Access Control) or RBAC (Role Based Access Control) access control mechanisms are implemented to ensure that data will be exchanged on the basis of business and security requirements and not at the user's discretion.

10.1.2 Access controls for applications, systems and networks shall be consistent with the information classification given to the data they process/transmit or store.

10.1.3 Authorisation to access and/or disseminate information and information systems shall be based on the 'need to know' principle and classification of the information (e.g. C4 Highly Confidential, C3 Confidential, C2 Internal, and C1 Public). Individual users will be granted access based upon a business justification and approval process. Access shall be restricted according to the job role's requirement to read, write, execute or delete information, data or software.

10.1.4 Relevant regulation, legislation and any contractual obligations regarding the protection of access to data or services shall be considered when granting access rights to a particular system/application.

10.1.5 Where common job roles exist across MAG, users shall be given access based on PoLP (Principle of Least Privilege).

10.1.6 The default access granting standard shall be a "deny-all" setting for all users and access only granted upon receipt of an appropriately authorised access request.

10.1.7 Appropriate authentication and password management shall apply to all normal users and administrators on all system components.

10.1.8 The addition, deletion and modification of user ID's, access rights, credentials and other identifier objects shall be controlled by the Information Services team, through appropriate procedures for User Identification, Access Requests and Password Management.

10.1.9 Managers, Information/Business Owners (IAOs / IAAs) are responsible for authorising access requests to their information assets in line with this Authentication & Access Control Standard and supporting procedures.

10.1.10 Any changes to system parameters that define the scope of access control systems shall be subject to the Information Services Change Management Standard and supporting processes.

10.2 Access Control

10.2.1 Every user shall be allocated a unique user ID. Generic or shared accounts are not allowed.

10.2.2 Each user account shall be protected with a strong password. Externally accessible solutions must incorporate a second authentication factor.

10.2.3 Users shall only be able to access front end layers, and must not have direct access to back-end systems.

10.2.4 Admin and Functional accounts must have an increased level of Security (compared to regular User Accounts), by ensuring that longer passwords (12-15 chars, min) are being used. Where possible, MFA should be enforced.

10.2.5 Any equipment in publicly accessible areas shall be IP55 and anti-vandal compliant.

10.3 User ID, Authentication & Accountability

10.3.1 Each individual requiring access to the MAG corporate network shall be individually defined, with each user individually recognisable to the system. Each new user at first logon shall be required to read and accept MAG's Acceptable Use Standard.

10.3.2 All access permissions shall be requested via the MAG IS Helpdesk, except for any hosted/managed systems where access is controlled by a third party or other MAG business operation.

10.3.3 The function (e.g. IS Helpdesk) responsible for granting, removing and restricting access permissions for information services and systems shall maintain accurate records of all access requests received, together with approval/rejections and activities undertaken. These records shall be auditable.

10.3.4 All MAG users (internal and external) will be assigned a unique ID before they are allowed access to the MAG network, applications and system components. No individual may use another person's user ID to gain access to the MAG network, applications and system components.

10.3.5 User ID's and credentials shall not be shared or disclosed to other users in order to gain access to the MAG network, applications and system components. Logon credentials shall not be shared with another user covering a role in the event of long-term absence (e.g. maternity leave).

10.3.6 In addition to assigning a unique ID, all MAG users will be authenticated to the domain via a password.

10.3.7 Remote access to the MAG network by employees, administrators and third parties will be subject to User ID/Password and token-based authentication to create a more secure two factor authentication mechanism.

10.3.8 Supplier user accounts are permitted in the MAG network environment. Supplier accounts are governed by this Standard and the MAG Acceptable Use Standard. High risk supplier access accounts should be disabled except when needed by the Supplier and monitored while in use.

10.3.9 Where supplier account access is required for data transfer and/or 24x7 support, continual access may be permitted with authorisation from the Head of Technical Operations and Infrastructure or MAG Information Security Team and where the account logon is monitored.

10.4 Password Management

10.4.1 Password management procedures shall be maintained by the MAG Information Services department to ensure that the allocation of passwords is controlled and password practises do not affect the integrity of MAG's information system environments.

10.4.2 Users shall be required to sign a statement as part of their terms and conditions of employment to keep personal passwords confidential and to keep any authorised group passwords solely within the members of the group.

10.4.3 User identity shall be verified before performing password resets. Procedures shall be documented outlining relevant work instructions around methods of verifying identity.

10.4.4 Temporary passwords shall be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic messages is to be avoided.

10.4.5 Temporary passwords for first-time use and resets shall be unique to an individual and not be guessable. Users shall be forced to change temporary passwords immediately after the first use.

10.4.6 Passwords shall never be stored in computer systems in an unprotected form. Passwords shall be rendered unreadable during transmission and storage on all system components using strong cryptography.

10.4.7 Default vendor passwords and accounts shall be altered before installation of systems or software onto the MAG corporate network.

10.4.8 Passwords shall only be known to the individual and shall not be written down or disclosed to another individual under any circumstances. Passwords shall not be inserted into email messages or other forms of electronic communication.

10.4.9 Passwords for the domain and individual applications shall be changed after a maximum period of 60 days.

Passwords shall meet the following complexity requirements for user accounts:

- At least 8 characters
- Does not contain "Administrator" or "Admin"; or easily guessable titles such as "Airport"
- Shall not contain any personal details, such as name, date of birth, phone number;
- Contains characters from all of the following categories:
  - Uppercase letters
  - Lowercase letters

  - Numbers
  - Non-alphanumeric characters
- Passwords shall be unique at each change and not follow a repeated pattern (e.g. MAG01, MAG02 etc.)
- If an account or password is suspected to have been compromised, it shall be reported to the IS Helpdesk immediately and all passwords shall be changed.
- User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from all other accounts held by that user.

10.5 Third Party Access

10.5.1 All third party access shall be authorised by an appropriate member of the Information Services department or local IAO or IAA and, if necessary, monitored. Third party access to MAG's information assets shall only be granted according to business need and identified risks. IAOs / IAAs shall specify access timeframes and be prepared to offer justification for such access. Accounts used by Suppliers for remote access shall be enabled only during the time period required to conduct the relevant approved activity. Strong Authentication will be required. Session information could be recorded, for monitoring purposes. Systems must force a timeout after a defined period of inactivity or after the access timeframe has been met. Remote Support accounts must be audited on a regular basis, at least once a year. The Infrastructure Manager is responsible for monitoring the remote access accounts when in use.

11. Information Systems Acquisition, Development and Maintenance

11.1 Security Requirements for Information Systems

11.1.1 The Third Party shall ensure that any new systems introduced into MAG's Information environment are compliant with PCI DSS (where applicable), the requirements of UK Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation (GDPR) and any other relevant legal and regulatory requirements.

11.1.2 Capacity requirements must take into account the business criticality of the system. Procedures must require information systems to be designed to cope with current and predicted information processing requirements. The Third Party shall ensure that capacity requirements are monitored and Third Party Systems and networks are regularly reviewed so that they are scaled accordingly.

11.1.3 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that where cryptographic controls are implemented, procedures for the use of cryptography and key management are in line with the MAG Data Encryption Policy, are securely managed using documented policy procedures, and key changes made under dual control.

11.2 Security in Development, Change and Support Processes

11.2.1 A policy document to outline a secure process for software development of software and systems processing MAG Information, whether in-house or outsourced, needs to be defined and maintained

11.2.2 Technical security standards (including secure build configuration) for applications and systems used in processing MAG Information must be defined, documented and maintained. New systems and applications must comply with these standards.

11.2.3 The Third Party shall ensure that change control procedures are agreed and documented between the Third Party and MAG; and that such documented procedures require that detail as to why the change was required and how and when the changes were executed are recorded and also include an emergency change process.

11.2.4 The Third Party shall notify MAG of any upgrades or configuration changes which will impact on the security of MAG Information, including (but not limited to) payment card information which as such may affect the PCI DSS compliance status of the Third Party and Services.

11.2.5 The Third Party shall ensure that back out procedures are documented prior to implementing any change.

11.2.6 The Third Party shall ensure that all changes for information systems, upgrades, and new software in relation to the Services have considered security control requirements, based upon the identified risks, and that these changes are tested prior to implementation.

11.2.7 The Third Party shall ensure that access to program source code is restricted and strictly controlled.

12. Incident Management

12.1 Policy and Procedure

12.1.1 The Third Party shall (and shall ensure that its Subcontractors shall) at all times maintain a security incident response procedure.

12.1.2 The Third Party shall ensure that mechanisms are in place to enable the types, volumes and costs of information security incidents to be quantified and monitored. Where required by MAG, the Third Party will provide such information regarding information security incidents to MAG.

12.1.3 The Third Party shall require all Third Party personnel (and any Subcontractor personnel) to report any observed or suspected security weaknesses in Systems or Services to the Third Party. The Third Party shall inform MAG immediately about any such weaknesses of which it becomes aware.

12.2 Reporting

12.2.1 In the provision of Services to MAG and as part of the security incident response procedure, if the Third Party becomes or is made aware of any contravention of the information security requirements under the Contract, or of unauthorised access to MAG Systems, MAG information or any MAG Systems including the MAG network, the Third Party shall (and shall ensure that its Subcontractors shall):

- immediately report the incident to the MAG Information Security Team;
- promptly provide MAG with a detailed written report setting out the details of and reasons for the contravention of the information security requirements and describing in detail any MAG Information, Systems and/or MAG Systems which have been accessed without authorisation;
- provide MAG, at no additional cost, with any assistance to restore MAG Information, the Systems and MAG Systems and any other assistance that may be required by the MAG;
- preserve evidence to include collection, retention and presentation of such evidence to The Information Security Team;
- promptly return to MAG any copied or removed MAG Information;
- comply with all reasonable directions of MAG; and
- take immediate remedial action to secure MAG Information, Systems and /or MAG Systems and to prevent reoccurrences of the same or similar contravention and provide MAG with details of such remedial action.

12.2.2 If either a criminal situation or a breach of Third Party policies and the requirements in the Contract occurs involving Third Party or Subcontractor personnel who are providing Services to MAG and such criminal situation or breach becomes known to the Third Party (or its Subcontractor), MAG must be notified as soon as practicable of the facts surrounding the same.

13. Business Continuity Management

13.1.1 The Third Party shall (and shall ensure that its Subcontractors shall) comply with MAG Business Continuity Policies as attached to the Contract or notified to the Third Party from time to time.

13.1.2 The Third Party shall (and shall ensure that its Subcontractors shall) align with the Business Continuity Standard ISO22301.

13.1.3 The Third Party shall ensure that a Business Continuity Plan is in place in relation to the provision of Services to MAG. The plan shall set out how business operations shall be restored following an interruption to or failure of business processes within a time period agreed to be acceptable by MAG.

13.1.4 The Business Continuity Plan shall include arrangements to inform and engage appropriate MAG personnel in its execution.

13.1.5 The Third Party shall test the Business Continuity Plan at least annually and shall report back to MAG on such testing where required by MAG.

13.1.6 The Third Party shall at least annually review and update, as necessary, the Business Continuity Plan and shall submit any proposed updates to the Business Continuity Plan to MAG for MAG's written, prior approval.

14.Compliance

14.1 Data Protection

14.1.1 The Third Party shall at all times ensure that it maintains and abides by an appropriate Data Protection Policy to safeguard MAG Information in accordance with the terms of the Contract, the UK Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation (GDPR) and any other applicable statute, regulation or industry code.

14.1.2 Where any MAG Information is intended to be transferred, stored or processed outside of the UK, the Third Party shall provide, for MAG written approval, full details of the locations, security arrangements and what information is to be transferred, stored or processed outside of the UK.

14.1.3 Where any elements of service delivery are proposed to be offshored, the proposal must be subject to a full information security risk assessment and must be approved by the MAG Information Security Team, and reviewed by Legal, before it can proceed.

14.1.4 The Third Party shall ensure that appropriate retention and secure deletion/destruction policies and procedures are in place for all MAG Information held. MAG may require a copy of the policies and procedures.

14.1.5 The Third Party shall maintain an information retention & destruction policy to ensure that MAG Information is retained for no longer than necessary and is protected from unauthorised or unlawful processing.

14.1.6 Where the Third Party is acting as a data processor for the Services, they must act only in accordance with MAG's instructions and approval.

14.1.7 The Third Party shall ensure that the storage and subsequent destruction of MAG Information is secure and in compliance with MAG's instructions. All items of equipment used in the provision of the Services containing storage media shall be checked by the Third Party to ensure that any MAG Information and licensed software has been removed or securely overwritten prior to secure deletion.

14.1.8 If MAG Information is to be shared with a Sub-contractor, the Third Party shall notify MAG in advance and provide MAG with a copy of the legal agreement in place.

14.2 Data Protection Controls

14.2.1 All data shall only be retained for the length of time that it is required with automated deletion built in wherever possible.

14.2.2 Users will be able to view an appropriate privacy notice and must give their consent before any personal information is collected, processed or stored.

14.2.3 Information must be encrypted at rest.

14.2.4 Backup tapes must be encrypted and stored securely.

14.2.5 Where applicable, the system must be able to extract personal data easily to provide in response to a request.

14.2.6 When relevant, a Privacy Impact Assessment will be completed.

14.3 Legal, Regulatory and Contractual Compliance

14.3.1 Legal, regulatory or contractual requirements must be complied with and taken into account in the processing of MAG Information. In particular this includes, but is not limited to compliance with the UK Data Protection Act 2018 (DPA), the EU General Data Protection Regulation (GDPR) and privacy requirements.

14.4 Compliance with MAG Policies and Standards

14.4.1 MAG Information processing systems including databases processing MAG Information must be checked on an annual basis to ensure they comply with relevant security procedures including this policy.

14.4.2 An annual report on the compliance of MAG Information processing systems against the relevant information security standard and this policy must be provided to the MAG Information Security Team.

14.5 Audit

14.5.1 The Third Party shall grant to MAG such access to the Sites used as is necessary to allow the MAG to perform its responsibilities or exercise its rights under the Contract and shall participate in information security reviews as and when reasonably requested by MAG.

14.5.2 If an investigation or audit is conducted by MAG or on behalf of MAG, the Third Party will ensure that all personnel shall cooperate with such investigators or auditors and, if requested, will make relevant personnel available for interview.

14.5.3 On or after termination of the Services, the Third Party shall grant MAG the right to perform reasonable audits and inspections of the Third Party and its Subcontractors for reasons of security, fraud and regulatory compliance in relation to the Services; or for reason of verifying the Third Party's compliance with the Contract. Equipment (where applicable) and data must be securely disposed of, in a way that ensures it cannot be recovered by any means. Examples include, hard drive shredding and/or low level formatting of all relevant drives.

14.5.4 If the Third Party has attained external validation or certification to any security industry standards, for example, this may include certification or standards such as ISO 27001, PCI DSS, SSAE 16, or any other audit standards which may contain security control assessments, the Third Party shall provide evidence of the relevant certification and/or Statement of Applicability upon request.

15. PCI-DSS Compliance (where applicable)

15.1.1 Where financial transactional functionality is (or becomes) a part of the Services, the Third Party shall comply with the latest version of PCI DSS requirements and provide evidence of PCI compliance through external certification or self-assessment declaration.

15.1.2 The Third Party shall maintain a written strategy for PCI DSS compliance in accordance with the Third Party Corporate Information Security Policy, which addresses each of the PCI DSS requirements, and shall assign responsibility for PCI DSS to a compliance function.

15.1.3 The Third Party shall ensure that a current network configuration diagram is produced and maintained to show clear information flows and to ensure that all connections are identified, including MAG's payment card transactions and any wireless networks.

15.1.4 The Third Party shall not disclose MAG's payment card transactions to any third party or entity, with the exception of where this is authorised by MAG under the provisions of the Contract or by prior written consent.

15.1.5 Upon request by MAG, the Third Party shall provide to MAG a written account of the scope of the environment that is included in the PCI-DSS assessment (e.g. Internet access points, internal corporate network) and identify any areas that are excluded from the PCI DSS MAG's payment card transactions environment.

15.1.6 Upon request, the Third Party shall provide to MAG written details around any gap analysis that has been produced either internally or by a PCI DSS Qualified Security Advisor (QSA). This shall include the provision of details of the most recent Self-Assessment Questionnaire or Report on Compliance.

15.1.7 Upon request by MAG, the Third Party shall provide to MAG written details of results of the last four quarterly network vulnerability scans.

15.1.8 Upon request by MAG, the Third Party shall provide to MAG, written details around any compensating controls employed by the Third Party to achieve risk mitigation in technical areas which do not meet the PCI DSS requirements.

16. Documents Required

16.1.1 The Third Party shall supply the following documents, policies and procedures upon request by MAG:

- High-level architecture diagram
- Information Security Policy
- IT/IS Organisation Chart
- Data Retention Policy
- Data Storage and Disposal Procedure
- Security Incident Response Procedure
- Business Continuity Plan
- Data Protection Policy
- Physical Security Policy
- Acceptable Use Policy
- Disciplinary Policy
- ISO27001 Certification
- SSAE16 Report
- PCI-DSS Certification
- SOC2 Report
- Recent penetration test report