Information Security Policy



Renewal date: 30 June 2027

Table of contents

Section		Page no.
1.	Introduction	3
	1.1 Purpose	3
	1.2 Expiry and renewal	3
2.	Information security	4
3.	Maintaining private clients' information	5
4.	General guidelines for all officers	6
5.	Password maintenance and protection	6
6.	Structure and control of passwords	8
	6.1 Types of access	8
	6.2 User / Client passwords	8
	6.3 The Administrator / The Super-User passwords	8
	6.3.1 The Administrator password operated jointly	9
	6.3.2 The Administrator password operated individually	9
7.	Protection against malicious software / hacking	10
8.	Data backup	11
9.	Email / user ID deactivation of outgoing employees	12
10.	Operating protocols for the Google sheets	13
Annex – A: List of authorized officers		15
Annex – B: The Administrator password operated jointly		16
Annex – C: The Administrator password operated individually		17
Annex – D: List of approved officers for the Google sheets		18

Section 1: Introduction:

1.1 Purpose:

The purpose of the Information Security (IS) Policy 'the Policy' is to ensure that the Company's information is a) secure at all times b) protected against anticipated threats to security or integrity and c) protected against unauthorized access that could result in harm / inconvenience to the client.

The Policy is applicable on all information which is:

1. Stored on the computers, storage drives and USBs.
2. Transmitted through emails.
3. Printed or handwritten on paper.
4. Communicated over the phone.

Although the Policy aims to protect confidentiality of the Company's information, efforts have been made to ensure that the information is timely available to all officers without causing disruption to the business processes of the Company.

It is the responsibility of the relevant departmental heads to ensure that all officers in their department are aware of the Policy. All breaches of information security, whether actual or suspected, shall be reported to the relevant department head and the Compliance Officer (CO). The relevant department head and the CO will investigate the matter and provide a report to the Board within 15 calendar days of reporting the incident.

All officers are required to follow the guidelines of this Policy in letter and spirit in order to ensure that all Company specific information remains protected at all times. Any violation of this Policy will be considered a part of 'Misconduct' as defined in the HR Manual.

The CO and IT officer are responsible for ensuring compliance with this Policy.

1.2 Expiry and renewal:

The Policy has been approved by all Board members and any subsequent amendments must be approved by the same authority. It is the responsibility of the CO to ensure that too much reliance is not placed on subsequent amendments and a revised IS Policy is issued on a timely basis once a number of amendments have been issued.

Section 2: Information Security:

It is important to understand that IS Policy of any company is dictated by the company's business model, the type of information maintained and the size of that company. Magnus is in the investment advisory / portfolio management business. It is not a deposit taking institution unlike commercial banks and CDC and is also not a transacting institution unlike brokers / dealers of securities. It is not a generator / producer of primary information of clients. The size of the Company is relatively small.

One critical information security risk that companies face is the loss or damage to their client's information. This risk is not critical for Magnus because the Company maintains / processes secondary information which is obtained from CDC, commercial banks and brokers / dealers of securities. The secondary information can always be reconstructed by Magnus in case of loss or damage to the same.

For Magnus, the most critical aspect of the information security is maintaining client confidentiality. Magnus has two categories of clients - private clients and institutional clients. The confidentiality of information for private clients is far more important than the institutional clients because the private client related information contains personal details of the individuals and their assets. This is not the case with the institutional clients where their information is on a fund level basis without any personal or individual asset details.

Considering the above fact, the Policy provides detailed guidelines for maintaining private clients' information in section 3.

Section 3: Maintaining private clients' information:

As mentioned in the previous section, the confidentiality of information for private clients is far more important than institutional clients. The Portfolio Management (PM) and the Finance teams are responsible for maintaining clients' data. The head of these two teams should make sure that the access to such information of the clients is restricted to those selected officers who need to know that information.

The following guidelines should be followed by all 'PCG Officers' in order to protect the clients' data from unauthorized access / use:

1. All attachments that contain personal information of the clients or have any information related to the portfolio should be password protected. The password to be used internally and by the clients will be the same. The password can only be communicated to the clients through a phone call or text message (no WhatsApp or email). For internal purposes, the password will be communicated / shared on the Group WhatsApp ID.
2. All clients' documents (except the Agreements and the PIR) will only provide initials of the clients and / or a specific client number (code) to be assigned at the time of signing Investment Agreement. This is not applicable to trade and settlement letters for discretionary clients.
3. All KYC forms (including but not limited to PIR and the Agreements) which contain clients' name and other personal details must not be saved in any laptop or computer which is not password protected.
4. All KYC forms whether it is a Word or a PDF file must be password protected.
5. The password should be same for all files of each client. The password will only be shared with the CEO, the CIO, the CFO, the CO, the PM head and other relevant officers of the PCG.
6. Hardcopies of all KYC forms (including but not limited to PIR and the Agreements) which contain clients' name and other personal details must be lodged in a bank locker in a sealed envelope. The envelope will only be labeled clients' code and initials. The documents must be lodged in the first week of each month. A separate bank locker should be arranged for all the PCG / SPG clients.
7. All client related documents / files must be stored in a separate / dedicated cabinet under lock and key. The keys should be under the control of the CO and the two senior most PCG officers.
8. The PCG officers should maintain their complete data in OneDrive[1].
9. The Officers should make sure that there is no loose paper containing clients' personal information on their desk at day end. All confidential documents are stored away under lock and key before leaving office. All the second keys should be with the CO and the CFO.

It is important to note that maintaining hard copies of clients' files is necessary for the SECP, rating agency, external and internal audit for assessing our controls, compliance and KYC standards.

The KYC documents (including but not limited to PIR and the Agreements) which contain clients' name and other personal details must not be kept in clients' files. The PIR and the Agreement for all clients should be saved on Z-drive with access restricted to a) the senior most officer in the PCG b) the CFO and c) the CO[1].

[1]Due to the COVID-19 outbreak, Magnus has implemented OneDrive – cloud based backup solution. All officers take backup on OneDrive accordingly.

Section 4: General guidelines for all officers:

The following guidelines should be followed by all 'Officers':

1. Laptops should be issued to the head of the PM, PCG, PA and SA departments, to be kept at home and used exclusively for office work.
2. USB ports of all officers (except team leaders and sub-team leaders) must be locked. Moreover, internal data transfer will be made through the OneDrive.
3. Outlook passwords shall not be shared with any officers except the team leaders.
4. Encrypted drives shall only be issued to the team leaders.
5. For emails received over the weekends, an automatic email response must be sent to all external parties, which must acknowledge the receipt of that email and specify that the reply on the query will be provided by the next working day[1].
6. Unauthorized use / transfer of any office related data is strictly prohibited, IT / Administrator will monitor such actions accordingly and strict action will be taken against such officers.
7. For time sensitive nature of work, office premises can be opened on weekends.
8. The name of PCG clients cannot be mentioned on WhatsApp.

Section 5: Password maintenance and protection:

Password protection is of foremost importance and all officers should follow the guidelines below to ensure sound security procedures:

a. Password used by the officers in the company should be strong and must meet the following minimum standards:

   i. Be at least eight to fourteen characters in length.
   ii. Contain at least one lowercase character.
   iii. Contain at least one number.
   iv. Contain at least one special character.
   v. Contain at least one uppercase character.
   vi. Cannot contain your first name, last name, or username.

b. The choice of password must not be your phone, cell phone, identity card or credit card number.

c. Passwords must not be shared with any unauthorized person. The authorized personnel for each password are defined in section 5.

d. Passwords will not be written down or stored offline or online which is easily accessible to anyone unless adequately secured.

e. Passwords will not be stored in a file on a computer system or mobile devices without encryption.

[1] This requirement specifically relates to the client team.

f. Passwords must not be sent through email or revealed over telephone. For overseas officer/s an exception to this rule applies. In such a case, the password will be communicated through WhatsApp or iMessage.

g. Officers should not use "Remember Password" option on any applications (for example, web browsers) except MS Outlook.

h. Officers should not hint at the content or format of the password.

i. In case an officer suspects that his password has been compromised, he should immediately change the password.

j. If the officer is an authorized personnel as per sub section 5.3.1 and 5.3.2 and suspects that his password has been compromised, he should immediately inform the CO about his perceived suspicion. The CO will take required measures and update the authorized personnel.

k. All officers should lock their PC / Laptop whenever they leave their work station. The keyboard shortcut for locking the PC is 'Windows + L'.

Section 6: Structure and control of passwords:

6.1 Types of access:

Every application or service has the following two types of access points:

a. User / Client:
   The Users / Clients have restricted access to the application as defined by the Administrator.

b. The Administrator / The Super-User:
   The Administrator or the Super-User Access has unrestricted access to the complete application and can make all types of changes, updates, and modifications in the application. This includes and is not limited to creating / deleting users, assigning rights and accessing all data.
   This access is only available to the CFO and CO.

6.2 User / Client passwords:

These passwords are personal responsibility of each officer and every officer will have his unique ID and a corresponding password. No officer will delegate his user authority to any other officer by way of sharing his credentials.

The following list of passwords fall under this category and must not be shared with any other officer:

i. PC / Laptop Windows login password.
ii. Official email account password (applicable on team leaders only).
iii. SHerp (Accounting software) user password.

If a supervisor requires using his junior team member's PC to extract a required file, he may follow one of the following steps:

i. Contact his junior team member to email the required file (from the junior's backup).
ii. Request CO having the OneDrive access to login as the Administrator on the relevant officer's cloud database and extract the file.

6.3 The Administrator / The Super-User passwords:

The Administrator or the Super-User passwords for applications or services can be termed both critical and non-critical in nature. Critical passwords will be operated jointly, whereas non-critical passwords will be operated individually.

The officer to whom the password is shared has the responsibility to not misuse the accessible information in any way or to communicate the password to other non-authorized officers, be it in negligence. If the authorized officer feels at any point in time that the password is suspected to have been compromised, he should immediately inform the Administrator.
The Administrators (the CFO and CO) has the rights to the password and is responsible for sharing the complete password with the authorized officers.

The license keys of all Microsoft products must also be readily available with the Administrators.

6.3.1 The Administrator passwords operated jointly:

The applications or services which are classified as critical must have a jointly operated Administrator password. The Administrator passwords can be operated by one officer from each two separate groups.

Groups	Number of officers	Password requirements
A	4	6 digits
B	4	6 digits

Please see list of authorized officers in Annex A.

Please note the following:

a) For simplicity, the password for both groups will be the same.
b) Group A will type in the first 6 digits and group B will type in the last 6 digits of password. The password must meet complexity requirements as mentioned in Section 4(a).
c) The passwords will be assigned by the Administrator. The authorized officers of group A cannot share passwords with officers of group B and vice versa.
d) The approved password for each group cannot be used for any other purpose.
e) Only the Administrator can change the passwords.
f) The Administrator can only be the CFO and CO.

The list of application or services under this category is provided in Annex B.

6.3.2 The Administrator passwords operated individually:

Some applications or services require frequent log-ins. This becomes cumbersome if the passwords are operated jointly. In such a case, the authorized officer will have access to the complete Administrator password in order to operate the applications or services.

The list of applications or services under this category is provided in Annex C.

Section 7: Protection against malicious software / hacking:

Information systems, software and data must be protected against the risks relating to malicious software (Malware). Malware may give partial or full control of the computer to the hacker.

The controls against Malware / hacking will be as follows:

1. Appropriate technical and procedural controls (including “antivirus” software, limited system access rights, security awareness and change management controls) must be in place to minimize the risks relating to malicious and other undesirable software.
2. The IT department is responsible for defining the technical architecture to protect the organization against malware risks subject to practical constraints and cost-effectiveness.
3. Approved antivirus software must be installed by IT department on all applicable IT platforms. The software must be configured by IT for optimum protection and updated promptly when new malware signatures etc. are released.
4. Email messages and attachments must be routinely and automatically checked for Malware before use. Antivirus controls should be implemented in multiple layers e.g. email gateways, servers and desktop / portable computers.
5. Unauthorized software must not be installed on the organization systems.
6. Suitable incident reporting, management and contingency measures must be in place to minimize the impact of, and recover efficiently from, any malware infections.
7. All storage devices / media (disks, CDs, DVDs, USBs, passport drives or any other media) must be screened for Malware before installing on the computers by the IT department.
8. While traveling, it should be strictly ensured that no public Wi-Fi connections are used by the officers on their laptops. This is important to protect laptops containing confidential client data. It is important to understand that public Wi-Fi connections do not have a password and are prone to hacking. Officers should use USB Wi-Fi device instead. However, Wi-Fi connections at hotels which are password protected are safe and can be used.

Section 8: Data backup:

Routine backup procedures and controls must maintain the integrity and availability of IT services, and protect the confidentiality of data on backup media:

1. Off-line backup copies of essential confidential information, software and databases must be taken regularly. Backups must be sufficient to enable essential information and software to be recovered efficiently following a disaster or media failure affecting the primary data or systems.
2. Backup processes should be automated where possible. The software used for Backup must be authorized and licensed.
3. Backup equipment (storage devices / server) and processes must be regularly tested by IT Officer in production to ensure that they can be relied upon for emergency use when necessary.
4. Off-site backups must be stored in a remote location chosen to minimize the chances of being affected by a physical disaster affecting the main location (e.g. a major fire, earthquake, flood, storm etc.).
5. Media containing backup and archive data must be stored at a physically separate secure storage facility at least 5-10 km away from the primary data storage.
6. Transportation of media to and from remote storage facilities must be authorized by the CFO and recorded in a secure log such that the location of all media can be determined reliability at any point.
7. Backup should be performed by trustworthy people preferably by CO and or IT Officer.
8. Two copies of data backup should be taken and maintained at different secured locker (ideally bank locker).
9. All officers must take full back-up of all files on the OneDrive. IT Officer is not responsible for the backup of files located on individual officers' hard drives[1].
10. The IT Officer must take back-up of all departed employees' data on a secure, encrypted portable drive. This drive will be stored in the Company's fireproof locker.

[1]Due to the COVID-19 outbreak, Magnus has implemented OneDrive – cloud based backup solution. All officers take backup on OneDrive accordingly.

Section 9: Email / User ID deactivation of outgoing employees:

The day an employee leaves Magnus, IT officer needs to take the following steps:

1. Obtain the email ID deactivation date from the concern team leader via final clearance checklist or through email (copy CO on that email).
2. Follow up with the team leader if he doesn't reply in 24 hours.
3. Follow up with CO after 24 hours of the date (replied by the team leader above) if the email address has been deleted / deactivated.

NOTE:

The User ID of all officers are linked with their email addresses. Disabling the User ID will automatically deactivate the email address. The team leader and IT officer must ensure that the backup of emails has been taken before deactivation of the User ID, otherwise the emails cannot be recovered. The process to take backup of emails is as follows:

1. Open Microsoft Outlook.
2. Click 'File', select 'Open & Export' and choose 'Import / Export'.
3. In Import and Export Wizard, select 'Export to a file' and click 'Next'.
4. Select 'Outlook Data File (.pst) and click 'Next'.
5. Select 'email address' in the top row. For example: xxxx.xxxx@magnusinvestments.com and check 'include sub-folders'. This will ensure that the back-up includes inbox as well as sent items and other folders.
6. Select the default location (…\Documents\Outlook Files\backup.pst) or provide custom location and file name (for example: Outlook[initials].pst) and click 'Finish'.
7. The creation of the .PST file will take the significant time depending on the size of mailbox.

Section 10: Operating protocols for the Google sheets:

Magnus will use the Google sheets to improve inter-departmental and intra-departmental coordination. Initially, the following five (5) files have been uploaded on Google sheets:

1. Meeting schedule.
2. Marketing follow-ups:
    a. Magnus Partners LLP.
    b. ICG business.
    c. PCG business.
3. Client details – Magnus Partners LLP.

The number of files may increase in the future to further improve the coordination within the organization.

Google sheets:

1. Meeting schedule:

    All proposed (unconfirmed) and confirmed internal / external meetings will be recorded on this Google sheet.

    Department heads, sub-team leaders of the PM team, and their designated juniors will have access to the meetings' schedule uploaded on this Google sheet. The list of officers with access to the meeting schedule has been approved by the CEO via email dated 15 June 2023. Please refer to annex D. Any subsequent additions and deletions will be approved by the CEO.

    All meetings (pending confirmation or confirmed) must be immediately updated on the Google sheets by the responsible officer. All officers must ensure the following protocol to record meeting details on the Google sheet:

    - **Existing PCG clients:** Meeting schedule will show the relationship number, and not the name.
    - **Existing / prospective partners in Magnus Partner LLP or prospective PCG clients:** Meeting schedule will just show the first name (and not the family name).
    - **Existing and prospective ICG clients:** Meeting schedule will show their full names.

    The purpose is to maintain confidentiality of names where the relationships are with specific individuals.

2. Marketing follow-ups:

    Magnus will maintain separate files for marketing follow-ups of different businesses:

    i. Magnus Partners LLP.
    ii. ICG business.
    iii. PCG business.

The purpose is to have real-time access to key points and follow-up items (if any) of our meetings with potential partners / clients. The key points will be updated for Magnus Partners LLP only. But the follow-up items will be updated for all three businesses. These Google sheets must be updated within 48 (forty-eight) hours of our meeting with the potential partner / client. These should be updated by the responsible officers attending the meeting or their designated officer/s.

The Google sheet for 'marketing follow-ups - ICG business' is not a substitute for the meeting notes and the continuing files being maintained by the PM Team. The PM Team will continue to document the key discussion / decisions of the meetings with potential ICG clients in their respective continuing files as per our usual practice. If the PM team believes that marketing follow-up data or any other data as per this new file is redundant and cumbersome, they can delete the relevant columns through a proper note after the approval of the CEO.

The access to these files will be on a need-to-know basis. The list of officers with access to the marketing follow-up files for different businesses has been approved by the CEO via email dated 15 June 2023. Please refer to annex []. Any subsequent additions and deletions will be approved by the CEO.

3. Client details – Magnus Partners LLP:

The Google sheet for 'Client details – Magnus Partners LLP' contains key details of the prospective partners we have contacted for Magnus Partners LLP.

The access to this file will be very limited because of the sensitivity of the data. The list of officers having access to the marketing follow-up files for different businesses has been approved by the CEO via email dated 15 June 2023. Please refer to annex D. Any subsequent additions and deletions will be approved by the CEO.

Gmail accounts:

Officers will create their personal Gmail IDs to access the above-mentioned Google sheets. This will allow the officers to update and make changes (if required). It is understood and expected that the officers will maintain confidentiality of these Google sheets.

Back-up of the data:

To avoid any loss of data and other incidents, the Head of IT / the Finance Team will download all of the above-mentioned Google sheets on a weekly basis (every Friday).

Master access:

The master access of all of the above-mentioned Google sheets will remain with the Head of IT, Head of Portfolio Management, and Head of Compliance. Only these officers will have the credentials (i.e., ID and Password) to the Gmail account of Magnus Partners LLP where the above-mentioned Google sheets are maintained. Furthermore, these officers can grant / remove access to / from any officers subject to the approval of the CEO.

Annex - A: List of authorized officers

Groups	Authorized officers
A	Yousuf Jamil, Hasan Moin, Akif Hasan and Umair Aslam
B	Imdad Ali, Noman Talha, Saad Pasha and Ali Hussain

Annex – B: The Administrator password operated jointly

The following is the list of application or services where the Administrator passwords are used jointly by authorized groups:

S. no.	Password description	Authorized groups	
		First 6 digits	Last 6 digits
1.	Encrypted backup drive (departed employee)	A	B
2.	IP telephony	A	B
3.	Dotster Website (Magnus Hosting)	A	B
4.	AD Server (Cloud)[1]	A	B
5.	SQL and App Server (Cloud)[1]	A	B
6.	Microsoft Exchange Online	A	B
7.	Amazon Web Services (AWS) (Arkad portal hosting servers)	A	B
8.	Comodo EV SSL	A	B
9.	Antivirus server[1]	A	B

[1]The Administrator password for AD server, SQL and app server, and antivirus server, is same because they are connected on Magnus domain.

Annex – C: The Administrator password operated individually

The following is the list of application or services where the Administrator passwords are used individually by authorized officer:

S. no.	Application / Services	Authorized officers
1.	NADRA Verisys	Hasan Moin and Saad Pasha
2.	Biometric thumb impression system	Imdad Ali, Sajjad Azeem and Ali Hussain
3.	SHerp administrator	Ali Hussain and Hasan Moin
4.	Biometrics thumb impression (PCG room)	Ali Hussain and Hasan Moin

Annex – D: List of approved officers for the Google sheets

The following table provides list of approved officers for different Google sheets:

S. no.	Officers	Meeting schedule	Client details – Magnus Partners LLP	Marketing follow-ups		
				Magnus Partners LLP	ICG business	PCG business
1	Nadeem Jeddy	✓	✓	✓	✓	✓
2	Riyaz Chinoy	✓	✓	✓	X	X
3	Umair Aslam	✓	✓	✓	✓	✓
4	Akif Hasan	✓	X	X	X	X
5	Yousuf Jamil	✓	X	X	✓	✓
6	Ali Hussain	✓	✓	✓	X	X
7	Hasan Moin	✓	X	✓	X	X
8	Hamza Imtiaz	✓	X	X	X	X
9	Maaz Habib	✓	X	X	X	X
10	Muhammad Anas	✓	X	X	X	X
11	Anus Ali Khan	✓	X	X	X	X
12	Muhammad Iqbal	✓	X	X	X	✓
13	Noman Talha Khan	✓	✓	✓	X	X
14	Muhammad Faizan	✓	X	X	X	X
15	Ammar Ali	✓	X	X	X	X
16	Imdad Ali	✓	X	X	X	X
17	Saad Pasha	✓	X	X	X	X
18	Rahul Raj	✓	X	X	X	X
19	Umer Khursheed	✓	X	X	X	X
20	Rozina Mushtaq	✓	X	X	X	X