GDPR INFORMATION SECURITY MANAGEMENT SYSTEM – CUSTOMER POLICY

1.Introduction

Allay Claims Limited has a responsibility to protect all client, corporate and all other information in accordance with the General Data Protection Regulations (GDPR) 2016. We are required to monitor all information being transferred by our employees to the public and all other organisations. Any transferal of data will be done in accordance with this policy.

2.Scope

This policy applies across Allay Claims Limited such that all staff will be made aware through induction training, general refresher training and through documentation. No employee will be exempt from this policy.

3.Data security:

3.1. It is Allay Claims Limited's policy to comply with all laws regulating computers and data protection. We minimise exposure to risk by adopting robust practices regarding the use of data or inappropriate, or illegal use of software.

3.2. Save in relation to reasonable e-mail and Internet usage and policy our employees are only permitted to use Allay Claims Limited's computer facilities to perform their job functions. We allow a restricted personal use policy which is subject to strict accountability.

3.3. To protect our client data staff are expected to keep their personal password confidential at all times and in accordance with password policy such that staff must not use personal data in their password, they should change their password regularly and must never share or divulge their personal password to any unauthorised person.

3.4. Staff are only authorised to use systems and have access to information which is relevant to their job and know that they should neither seek information nor use systems outside of this criterion.

3.5. Software issued by Allay Claims Limited for your use is licensed to Allay Claims Limited and is protected by copyright law. Neither Allay Claims Limited nor any member of staff may make copies or distribute software that has been copied.

3.6. Staff are not permitted or authorised to:

- 3.6.1. install software onto Allay Claims Limited's computers without first obtaining permission to do so and, because of the risk to Allay Claims Limited's computers of any computer virus staff are expected to raise any issue which may relate to a computer virus with the IT Manager.
- 3.6.2. download any 'copyright' material onto any device that is supported by our IT network. This includes downloading 'copyright' material onto a personal mobile phone where access to Allay Claims Limited's Wi-Fi has been granted.
- 3.6.3. download, onto any device that is supported by Allay Claims Limited's network, any software for which Allay Claims Limited does not have a valid license. You must not download any such software without first obtaining the permission of the IT Manager.

3.7. Allay Claims Limited operates a secure WiFi service that is restricted and only accessible via either the Operations Manager or the IT Manager. Allay Claims Limited reserves the right, in its sole discretion, to allow you to access Allay Claims Limited's Wi-Fi for the personal use of either staff or visitors . Where access is granted the password is not provided but is activated by authorized staff only and, where a password is made available (highly unlikely) the individual is advised that they are under a strict obligation not to share the relevant passwords or login details with other members of staff or other visitors. Accessing and using Allay Claims Limited's Wi-Fi shall be restricted to only authorised and designated breaks.

3.8. All laptops with company data have full disk encryption enabled using appropriate OS software.

3.9. Only authorised staff are permitted to use USB Mass Storage Devices within Allay Claims Limited, as determined by the IT department, backed up with suitable job justification. Staff are advised to perform an Anti-Virus scan on any device after is has been plugged into any machine and where possible the USB device should be encrypted if the device is to be used to transport any company data.

4.Internet and E-mail Usage:

4.1. Allay Claims Limited's computer system contains e-mail and Internet access facilities which are intended to promote effective communication within Allay Claims Limited and with clients and contacts relating to its business. Both systems are therefore used for that purpose.

4.2. Allay Claims Limited permit limited personal messages sent via e-mail, but these must respect the primary purpose of the e-mail system. Our policy states that our e-mail system should not be used for a purpose detrimental to the job responsibilities of a member of staff, for spreading gossip, for personal gain or in breach of any of Allay Claims Limited's policies.

4.3. All individuals representing Allay Claims Limited's best practice must refrain from including bad language and/or references to inappropriate or offensive content within any message sent on the e-mail system. Confidential information is not sent externally by e-mail without express authority and unless the messages can be lawfully encrypted.

4.4. Staff are permitted reasonable use of our Internet facility. This is limited to break times and to the accessing of appropriate sites. We have a policy on the accessing of unsuitable sites which is viewed seriously by Allay Claims Limited and can lead to disciplinary action.

4.5. Allay Claims Limited has the right to retrieve the contents of e-mail messages and to examine computers in relation to Internet access for monitoring whether the use of the e-mail and Internet systems is legitimate, to assist in the investigations of wrongful acts or to comply with any legal obligation.

4.6. Allay Claims Limited instruct staff that when they leave their PC unattended or on leaving the office they ensure any PC is locked or secured to prevent unauthorised users accessing our system and our data.

4.7. If, as a customer of Allay Claims Limited you receive an e-mail message which has been wrongly delivered you should notify the sender of the message by redirecting the message to that person who will notify out Data Protection Officer who will then contact you to advise you of any action required. In the event the e-mail message contains confidential information you must not disclose or use that confidential information.

4.8. Misuse of the e-mail or Internet system in breach of this policy is taken very seriously by Allay Claims Limited. If any misuse is bought to our attention that constitutes misconduct it will be dealt with within the framework of Allay Claims Limited disciplinary procedure. Misuse of the e-mail system by transmission of any material in any of the following categories automatically constitutes gross misconduct:

- defamatory;
- offensive or obscene;
- untrue or malicious;
- racist or otherwise contrary to Allay Claims Limited's Equal Opportunities Policy
- protected copyright material.

5.Staff use of own device

Staff are fully briefed on the company Computer and Data Protection policy, with regards to Data Loss Prevention. Staff are aware that our IT department has the right to undertake audits on staff equipment that accesses the organisations data to ascertain whether or not this policy is being adhered to.

6.Sensitive Information

Allay Claims Limited operate a policy on the management of Sensitive information which is governed by the level of the Confidentiality in question and is marked appropriately in accordance with policy.

7.Virus Protection

All PC and Servers are vulnerable to intrusion by viruses without sufficient protection these devices could become infected and all information on these machines vulnerable to corruption, being stolen and/or deleted.

Allay Claims Limited has a responsibility to clients, employees and third parties to protect data from such a threat. We maintain strict guidelines to protect the company from viral and worm contamination and provide the means to minimise disruption and business impact should preventative measures fail.

Our IT Department operates and maintains up to date effective anti-virus software on all computer systems that are liable to attack from malicious software. All networked PCs are updated with the latest applicable virus definition files daily on start up. Virus protection of computers that are not networked is also maintained. Provision of this requirement is made by our IT Department.

8. Responsibility

It is the responsibility of each Line Manager at Allay Claims Limited to ensure this policy is deployed within their area of responsibility.

9. Customer Care Contact

If as a customer of Allay Claims Limited, you have any concerns relating to any aspect of our Information Security Management System you should contact the Data Protection Officer Mydata@allay.co.uk