S

1. Introduction

This document sets out the Company name>> (the "Coprotect the Company's convironment and any and from damage and threats where the Company's convironment and any and from damage and threats where the Company's convironment and any and from damage and threats where the Company's convironment and any and the Company's convironment and any and the Company's convironment an

2. Key Principles

- 2.1 All IT Systems are to
- 2.2 All IT Systems are Policies.
- 2.3 All employees of the the IT Systems inclu (collectively, "Users" must adhere to and others.
- 2.4 All line managers me must adhere to and paragraph 2.3.
- 2.5 All data stored on IT all relevant parts
 Legislation" means a but not limited to, the Regulation ((EU) 20 England and Wales, the European Union Privacy and Electror any successor legisla
- 2.6 All data stored on IT not limited to, persinformation) [with reappropriate>>]. All accordance with its of
- 2.7 All data stored on I legitimate need for a
- 2.8 All data stored on IT and/or processing.
- All data stored on corruption.
- 2.10 All IT Systems are upgraded by <<inser or by such third par authorise.

In by all employees of <<insert ompany as a whole in order to rices, infrastructure, computing ment (collectively, "IT Systems") deliberate, or accidental.

authorised access.

npliance with relevant Company

all third parties authorised to use contractors and sub-contractors are familiar with this Policy and

under their control and direction at all times as required under

aged securely in compliance with Legislation. "Data Protection ction and privacy laws including, n of the General Data Protection"), as it forms part of the law of Ireland by virtue of section 3 of he Data Protection Act 2018, the ulations 2003 as amended, and

sified appropriately (including, but personal data, and confidential sifcation system/procedure etc. if st be handled appropriately in

lable only to those Users with a

ted against unauthorised access

protected against loss and/or

tained, serviced, repaired, and partment>> (the "IT Department") partment may from time to time

- 2.11 The responsibility for stored thereon (inc confidentiality of that otherwise.
- 2.12 All breaches of secthereon shall be Department. [Any be personal data shall be and contact details>>
- 2.13 All Users must report or to the data stored concerns relate in a [instead] be reported

3. IT Department Responsibi

- 3.1 The IT Manager, <<ii the following:
 - a) ensuring that compliance w
 - b) ensuring that implemented Company's sappropriate,] Company's se
 - c) ensuring that
 Policy and o
 rules whether
 the Data Prot
- 3.2 The IT Staff shall be
 - a) assisting all U
 - b) providing all matters and u
 - c) ensuring that are appropria responsibilitie
 - d) receiving and taking appropressive reports relate
 - e) taking proacti security proce
 - f) assisting the Company and any changes
 - g) ensuring that Systems at i backups are backups shou

ty of all IT Systems and the data to, the security, integrity, and partment unless expressly stated

IT Systems or any data stored rently investigated by the IT known or suspected to involve Protection Officer, <<insert name

ncerns relating to the IT Systems the IT Department. [If any such , such concerns must [also] OR officer.]

details>>, shall be responsible for

sessed and deemed suitable for ity requirements;

thin the Company are effectively working in consultation with the nd Data Protection Officer, as come of such reviews to the

are of the requirements of this regulations, and other relevant orce including, but not limited to, computer Misuse Act 1990.

ving:

nd complying with this Policy;

upport and training in IT security

rels of access to IT Systems that ng into account their job role, ity requirements;

ating to IT security matters and [including, in the event that any ng the Data Protection Officer];

e, to establish and implement IT rareness;

oring all IT security within the tion to implement this Policy and tuture: and

en of all data stored within the IT <insert interval>> and that such ion [onsite] AND/OR [offsite]. All <insert type(s) of encryption>>].

4. Users' Responsibilities

- 4.1 All Users must compusing the IT Systems
- 4.2 All Users must use the IT Syster any UK law whether
- 4.3 Users must immedia relate to personal di concerns relating to t
- 4.4 Users must immedi problems (including, which may occur on
- 4.5 Any and all delibera handled as appropria

5. **Software Security Measure**

- 5.1 All software in use of systems, individual solution and all intermediate release Department. This properticular major releases of tware update is release, falling within scope of this provision.
- 5.2 Where any security fixed immediately or such time as the sec affects, is likely to af Protection Officer shadows.
- 5.3 No Users may insta supplied on physical of the IT Manager. A IT Manager and may risk to the IT System agreements to which
- 5.4 All software will be in an individual User is Such written permis and onto which comp

6. Anti-Virus Security Measu

6.1 Most IT Systems (in suitable anti-virus, fi such software will b definitions. of this Policy at all times when

n the bounds of UK law and must tivity which is likely to contravene ce.

ment [(and, where such concerns Officer)] of any and all security

partment of any other technical rare failures and software errors)

s of this Policy by Users will be disciplinary procedures.

ling, but not limited to, operating firmware) will be kept up-to-date tes, patches, fixes, and other the sole discretion of the IT d to upgrading software to new sion 2.0), only to updates within a 0 to version 1.0.1 etc.). Unless a e it will be classed as a major are procurement and outside the

software that flaw will be either ndrawn from the IT Systems until ely remedied. [If the security flaw ffect any personal data, the Data elv.]

own, whether that software is lownloaded, without the approval Users must be approved by the that installation poses no security ion would not breach any licence bject.

ems by the IT Department unless on to do so by the IT Manager. which software may be installed by be installed.

d servers) will be protected with le internet security software. All the latest software updates and



6.2 All IT Systems prote scan at least <<inser

6.3 All physical media (
Users for transferrin
transferred. Such v
connection / insertic
Manager].

- 6.4 Users shall be permi the approval of the I system must be scar
- 6.5 Any files being sent on physical media, scanned for viruses appropriate. [All ema
- 6.6 Where any virus is of the IT Department (automatically fixes the and all necessary at may involve the te Wherever possible a [immediately] OR [w
- 6.7 [If any virus or othe affect any personal of immediately to the D
- 6.8 Where any User deli IT Systems this will Act 1990 and will be procedures.

7. Hardware Security Measur

- 7.1 Wherever practical, securely locked whe in use or not (with at smart card, door cod Users must not allo reason.
- 7.2 All IT Systems not in to, servers, networ located, wherever pound/or in locked comembers of the IT D
- 7.3 No Users shall have Users (including spermission of the I problem with such I reported to the IT De to rectify any such cases, instruction an
- 7.4 All non-mobile devi

re will be subject to a full system

s or disks of any kind) used by anned before any files may be performed [automatically upon ne User] OR [by the IT Staff /

cloud storage systems only with vnloaded from any cloud storage e download process.]

the Company, whether by email, shared cloud storage) must be part of the sending process, as ed automatically upon sending.

must be reported immediately to en where the anti-virus software partment shall promptly take any em. In limited circumstances this affected computer or device. mputer or device will be provided >>] to limit disruption to the User.

ely to affect, or is suspected to pove, the issue must be reported

malicious software or virus to the nce under the Computer Misuse under the Company's disciplinary

cated in rooms which may be briate cases, at all times whether anted access by means of a key, ess to such locations is restricted, cess to such locations for any

 Users (including, but not limited network infrastructure) shall be ecured, climate-controlled rooms accessed only by designated

is not intended for normal use by above) without the express mal circumstances, whenever a by a User, that problem must be imstances should a User attempt oress permission (and, in most Manager.

limited to, desktop computers,

workstations, and physically secured i design of the hardw tampering with or the

- 7.5 All mobile devices smartphones) provide securely and handle are to be left unatten suitable container. Unabile devices from private homes or Cola vehicle it must be compartment.
- 7.6 The IT Department s All IT Systems shall the asset register.

8. Access Security

- 8.1 Access privileges for levels of authority wi Users shall not be grare not reasonably re
- 8.2 All IT Systems (and laptops, tablets, and or passcode, or such may deem appropri considered secure. (be used.
- 8.3 All passwords must,
 - a) be at least <<
 - b) contain a con spaces / syml
 - c) be changed a
 - d) be different fr
 - e) not be obviou dates, memoi
 - f) be created by
- 8.4 Passwords should to should a User share and the IT Staff. No anyone at any time reason to believe the should change their of security to the IT I by an unauthorised in
- 8.5 If a User forgets thei
 The IT Department v
 to the IT Systems v

ver possible and practical, be locking mechanism. Where the ases shall be locked to prevent

nited to, laptops, tablets, and should always be transported nces where such mobile devices of dinside a lockable case or other easonable efforts to avoid such at any location [other than their such mobile device is to be left in 1d, where possible, in a locked

asset register of all IT Systems. responding data shall be kept on

tetermined on the basis of Users' e requirements of their job roles. Systems or electronic data which of their job roles.

ices including, but not limited to, rotected with a secure password g-in system as the IT Department all forms of biometric log-in are roved by the IT Department may

outer, or device allows:

ers long;

lower case letters / numbers /

erval>> days;

d;

birthdays or other memorable laces etc.); and

User. Under no circumstances yone, including the IT Manager ely asked for their password by should be refused. If a User has s obtained their password, they and report the suspected breach personal data could be accessed ction Officer].

e reported to the IT Department. eps to restore the User's access suing of a temporary password



which may be fully of for resolving the is immediately upon the

- 8.6 Users should not write User cannot remem locked drawer or in a should passwords be to a computer display
- 8.7 All IT Systems with touchscreen etc.) s protected screensay inactivity. This time disable the screens disrupt any other processing).
- 8.8 All mobile devices smartphones) provid after <<insert time p other form of log-in period.
- 8.9 Users may not use the IT Systems with software must be rea job role and must b where such access r Data Protection Office
- 8.10 [Users may connect tablets, and smartp appropriate>>] Con Department. Any ar Department governir Company network r devices shall be sub (including, but not lin the Company netw Department shall res any such devices wit

9. **Data Storage Security**

- 9.1 All data, and in pai passwords and I<<in
- data, should be store
- 9.3 No personal data sh limited to, laptops, ta with all instructions a and for no longer tha
- No data, and in p 9.4

ember of the IT Staff responsible must be set up by the User the IT Systems.

possible to remember them. If a ld be stored securely (e.g. in a ase) and under no circumstances s to see (e.g. by attaching a note

devices (e.g. mouse, keyboard, ere possible, with a password fter <<insert time period>> of ed by Users and Users may not screensaver will not interrupt or on the computer (e.g. data

nited to, laptops, tablets, and I be set to lock, sleep, or similar, uiring a password, passcode, or ar. Users may not alter this time

allow outside parties to access nt of the IT Manager. Any such User for the performance of their eared by the IT Manager [and, cessible by the outside party, the

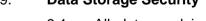
iding, but not limited to, laptops, rt specific network name(s), if ct to the approval of the IT equirements provided by the IT devices when connected to the times. Users' use of their own v. all relevant Company Policies those devices are connected to art of the IT Systems. The IT t the immediate disconnection of

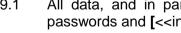
hould be stored securely using >>] data encryption.

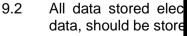
edia, and in particular personal x, drawer, cabinet, or similar.

mobile device (including, but not whether such device belongs to nal written approval of the Data approval, strictly in accordance at the time the approval is given,

should be transferred to any







the Company or oth Protection Officer ar computer or device p is a contractor or su User has agreed to and the Data Protect User unless the User in question behalf of the Company and that ompany's Data Protection Policy

10. Data Protection

- 10.1 All personal data (a held, and processed strictly in accordance provisions of the I Protection Policy.
- 10.2 All Users handling dand must comply wit at all times. In particular
 - a) All emails coutype(s) of end
 - b) All emails cor
 - c) Personal da transmission circumstance
 - d) Personal data is a wired alte
 - e) Personal dat received, sho stored secure associated th deletion>>];
 - f) All personal removable elemarked "conf
 - g) Where any co screen and the period of time leaving it.
- 10.3 Any questions relat Protection Officer,] <

11. Internet and Email Use

- 11.1 All Users shall be s Company's Commu Systems.
- 11.2 Where provisions in ensure IT security requirements imposured by take such

Protection Legislation) collected, e collected, held, and processed e Data Protection Legislation, the tion and the Company's Data

the Company shall be subject to, company's Data Protection Policy pply:

ust be encrypted [using <<insert

ist be marked "confidential";

d over secure networks only; ks is not permitted under any

l over a wireless network if there practicable;

y of an email, whether sent or rom the body of that email, and ld be deleted. All temporary files eleted [using <<insert method of

d physically, including that on ransferred in a suitable container

ta is being viewed on a computer is to be left unattended for any he computer and screen before

hould be referred to [the Data t details>>.

mply with, the provisions of the ernet Policy when using the IT

additional steps to be taken to t or email over and above the ons, Email and Internet Policy,

12. Reporting IT Security Brea

- 12.1 Subject to paragrap known breaches sha OR [the IT Departme
- 12.2 [All concerns, questi personal data shall be shall handle the ma Policy.]
- 12.3 Upon receiving a que within <<insert period level of risk associated it. Department deem
- 12.4 Under no circumsta breach on their own Protection Officer, a security breaches un the IT Department.
- 12.5 All IT security breach under the IT Departn

13. Policy Review

The Company shall review t as required in order to en questions, concerns, and communicated to the IT Ma Data Protection Officer, <<ir

14. Implementation of Policy

This Policy shall be deeme shall have retroactive effect this date.

This Policy has been approv

Name: <<insert f

Position: <<insert r

Date: <<insert of

Due for Review <<insert d

by:

Signature:

estions, suspected breaches, or ely to [<<insert specific name>>]
OR [a member of the IT Staff].

s, or known breaches that involve the Data Protection Officer who the Company's Data Protection

breach, the IT Department shall, including, but not limited to, the tke any and all such steps as the the issue.

tempt to resolve an IT security the IT Department [(or the Data may only attempt to resolve IT d with the express permission of,

y the IT Department or by a User fully documented.

<<insert interval>> and otherwise
-to-date and fit for purpose. All
ng to this Policy should be
nd contact details>> [and/or the
etails>>].

rt date>>. No part of this Policy y to matters occurring on or after