Data Security Policy and Disaster Recovery Plan

Preamble and Application

1 This Data Security Policy is applicable to all work undertaken by *acl* consulting. "Work undertaken by *acl* consulting" is defined as any work that is marketed, reported upon or invoiced under the aegis of *acl* . It is not intended to constrain individual Associates in their private practice, although all that is set out here is regarded as good practice and commended to all Associates.

2 The number of high profile losses of public data in recent years has been considerable. Loss of client data is always embarrassing and can sometimes be fatal either for the project or for the client relationship. In extreme cases it can leave individual liable to civil or criminal action.

3 There are two specific dangers that have to be guarded against:

- irreplaceable loss of data vital to a project or vital to the continuing effectiveness of *acl* consulting
- confidential or sensitive data falling into the wrong hands.

In our work, the first may be seen as more likely. However the second is also a possibility and in many ways has the more severe consequences.

4 Although most data risks apply to computer data, loss of information on paper (including, for example, notes of interviews and meetings and responses to questionnaires) can also be serious and this policy applies to paper-based data also.

5 Every effort has been taken to ensure that this policy is proportionate to the risks involved. Most of the data we handle does not carry a national security classification or a high financial transaction risk, and it is acknowledged that precautions applicable to data at this level of risk – key operated secure computers, dual password systems requiring two individuals to access – are not appropriate to us.

6 However it goes without saying that when individual assignments require a higher level of security than is suggested here then the requirements of this higher level must be adhered to.

7 This policy consists of mandatory instructions and "good practice" advice.

Guarding against loss of data; data recovery

8 Regular backups must be taken of all computer data, and these backups stored off site.

9 Backups can be taken by copying data to removable media, and storing these media in a safe off-site location, or by using an automated Web-based service.

10 Ideally backups should be taken daily, particularly of any client information that would be difficult to reconstruct. The transfer of backups to off-site locations does

not need to be on a daily basis provided there is confidence that any data lost can be reconstructed, e.g. from source material. Of course the cost of any such reconstruction (in time lost retyping and rewriting) is borne by *acl*.

11 Where backups are stored off-site, the security of their storage should be taken into account. If they are stored in an insecure location then the data on them should be encrypted using one of the recognised standards.

12 Where backups are taken by an automated Web-based service, then full notes concerning logging into the service (with passwords if applicable, and any software required) must be stored off-site in a safe location. Keeping information about restoring data to a computer purely on the computer itself negates any value in the backup, for obvious reasons. It is also important to understand how the data restoration process works.

13 It is not necessary to back up, or store offsite:

- data supplied by clients from their own maintained databases, provided it is certain the client will continue to maintain the data. Some databases *acl* works with are very large and would swamp the capacity of off-site storage and broadband connections if backed up regularly
- operating systems, programs and utilities

However it is worth ensuring that program disks etc. are to hand should programs need to be reloaded on a new computer in order to use restored data.

14 In this connection it should be borne in mind that any new computer is almost certain to use Windows Vista, and not all programs that run under Windows XP will necessarily run on a new computer.

Good practice in maintaining computers

15 Viruses and other malware can easily bring down a computer, and can in some circumstances permit third parties to access data. Sending a virus-infected file to a client can have equally serious consequences. All computers must therefore have installed on them effective up-to-date antivirus software, backed up with a current subscription. Firewalls are also strongly recommended.

16 If viruses or malware are detected on any files sent to a client, the client must be immediately notified. If viruses are found on files *from* a client, then again the client should be advised of this.

17 Computers should be set to install operating system updates distributed by the manufacturer automatically, since many of these are responses to identified security weaknesses. If automatic installation is not selected, then all security responses should be manually installed

18 Early attention should be paid to developing instabilities in a computer or its operating system. Having a standby computer (which may be a laptop) is recommended. Duplicating programs and current data onto the standby computer

periodically can bring reassurance, if it does not contravene programme licensing arrangements (but see below for further reference to laptops).

Guarding against data falling into the wrong hands

19 Desktop computers used for *acl* business should be kept secure. Use of the Windows “user accounts” function to set up password access is strongly recommended, and is mandatory if sensitive information is being stored on the computer (unless passwords are used to protect individual documents). Passwords should be changed regularly.

20 Laptops pose particular risks if they are taken into the field. Within reason, only data relevant to current assignments should be maintained on a laptop (unless it is the only computer available), and “user account” password protection should be implemented if at all possible.

21 Particular care should be taken when taking laptops on public transport. Having one bag for both laptop and work papers reduces the likelihood of the laptop bag being “forgotten”, and not using an obvious “laptop case” reduces the likelihood of theft. It is also good practice to be aware of who else may be able to view the laptop screen.

22 Memory sticks in the field pose particular dangers, both for loss and for their potential to transmit viruses and malware. If a memory stick is in use for a presentation, consider having only that presentation on the stick. If a memory stick is being used as a backup, it should be encrypted.

Data loss

23 It is *acl* policy that all cases of data loss are reported to clients who might be significantly affected, unless it is *certain* that the loss involved the destruction of the data carrier. (For instance, the failure of a computer or hard drive or other media where the physical media is still in one’s possession does not count as “loss” in this context.) Loss or theft of valuable equipment should also be reported to the police.

24 Loss of data protected by encryption or other security measures should be reported together with details of the measures taken. In most cases this will provide sufficient reassurance to the client that no future risk is involved.

25 No report need to be made to the client if “failed” hardware is successfully replaced and backed up data restored to it. This is a matter for *acl*.

26 In this context, care should be taken over disposing of unwanted computer equipment (whether in running order or not). Tests have shown that much of the data once held on a hard disk can be reconstructed, even if “deleted”. The safest option is physically to destroy the hard disk before the computer is disposed of.

Safety of physical assets and disaster recovery

27 *acl* Associates and Principal Associates are required to give careful consideration to their plans for recovering from any disaster that may affect their ability to deliver services or projects for which *acl* is contracted. These plans should include evacuation plans in case of emergency and plans for surviving interruptions to public services and utilities.

28 It is acknowledged that *acl* Associates and Principal Associates work largely from home, and in different local circumstances, so the nature of these recovery plans must be for individuals to determine.

29 It is also acknowledged that the swiftest and simplest response to the likely effect of a disaster on an *acl* project is to transfer work to another unaffected Associate or Principal Associate. At the very minimum, the advice of the Project Manager or another Principal Associate should be taken.

30 “Disasters” in this context should be taken to include medical, family or other personal emergencies that might affect an individual’s capacity to deliver contracted services.

31 It is also recognised that the individual affected will need time to respond to the disaster and its personal effects before “returning to work” can be considered, and all Associates and Principal Associates undertake to support the individual affected during this time.

32 It goes without saying that no personal risks should be run in an attempt to protect or recover data, equipment or other materials, even if they are client property. This point must be clearly understood.

33 On being notified of a disaster likely to affect project delivery, the project manager (or other Senior Associate if it is the project manager that is affected) should immediately confer with colleagues to establish how the project(s) affected will continue. Usually, it will be possible to re-schedule work between the existing team. Should this re-scheduling cause a delay, or should additional team members need to be introduced to cover the absent colleague, then the client must be notified promptly.

34 Physical records of fieldwork, client papers and other physical assets should be held as securely as circumstances permit, bearing in mind the likely risks involved. In general, paper records of the assignments we undertake are not at significant risk from casual theft, however, and police advice is that their over-elaborate protection (in conspicuously locked cabinets and drawers) may actually contribute to their risk of loss and destruction.

35 *acl’s* practice of circulating notes of all fieldwork, and indeed all work in progress (which will in any case have been backed up by the individual concerned) should ensure that these records are not lost in the disaster.

Compliance

36 Compliance with this policy is mandatory, and a Project Manager should hold copies of this Policy initialled by each member of his team.

37 To establish and maintain good practice, Project Managers should from time to time enquire of their colleagues:

- what arrangements have been made for secure offsite backup of data
- the extent to which IT equipment is protected either physically or through the use of passwords
- what his or her disaster recovery plans are
- whether the colleague wishes to raise any queries concerning the content of this policy.

V2.2
November 2013