

DGL CONSULTANTS, LLC INFORMATION SECURITY POLICY

OBJECTIVE

Our information protection policy sets out our commitment to protecting client data and how we implement that commitment with regards to the collection and use of client data.

POLICY

The policy's goal is to protect client informational assets against all internal, external, deliberate and/or accidental threats. We are committed to:

- Ensuring that we comply with the information protection principles, as listed below.
- Ensuring that information is collected and used fairly and lawfully.
 - Confidentiality of data will be assured.
 - Integrity and availability of data for business purposes will be maintained.
 - Legislative and regulatory requirements will be met.
- Processing client data only in order to meet our operational needs or fulfill legal and contractual requirements.
- Establishing appropriate retention periods for client data.
- Ensuring that data subjects' rights can be appropriately exercised.
- Providing adequate security measures to protect client data.
- Ensuring that all queries about data protection - internal and external – is dealt with effectively and promptly.
- Data security training will be met.
- Information and data will be protected against any unauthorized access.
- All actual or suspected information and data security breaches will be reported and thoroughly investigated.


PROTECTION PRINCIPLES

Our data and information protection principles:

- Client data shall be obtained with the purpose of completing our contractual obligation to the client, and shall not be further processed in any manner incompatible with that purpose.
- We use good common-sense practices to protect client information with strong encryption:
 - Client confidential data is stored on a stand-alone computer not connected to the Internet or a local area network (LAN). Windows Encrypting File System (EFS) is built into the OS and enabled for directories containing secure data.
 - Client data shall be sent back and forth in encrypted format. We email client data using secure email or with WinZip that supports 128- and 256-bit key AES encryption.

- Client data shall not be kept for longer than is necessary to complete our contractual obligation to the client. As such, all client data will be deleted 90 days after the client's project has been completed:
 - We destroy paper records using a cross-cut paper shredder.
 - We hold media and its contents closely; we don't share it inappropriately and we return it to an appropriated locked space when we are done.
 - We destroy other records in media-appropriate ways, such as erasing files using Tolvonen Eraser using DOD 3-pass erasing standard or if unable to be erased because it is broken, we destroy by physical breakage.
- All security incidents need to be identified, reported, investigated and monitored to ensure that reaction is appropriate to any actual or suspected incident relating to information systems and data within our custody. We log all incidents. Dependent on the severity and identified impact of the incident, we shall notify clients verbally and in writing until the incident is resolved, either temporarily or permanently.

DGL Consultants, LLC
3492 Hill Circle
Colorado Springs, CO 80904
Tel. 719-634-7041

By_  _____

Donald G. Lariviere
Principal

Date: June 27, 2013