DLD Group Inc.

Privacy Policy

Our Commitment to Privacy

Protecting the privacy and confidentiality of personal information is an important to DLD Group Inc. (hereafter referred to as "DLD"). Collecting, using, and disclosing personal information in an appropriate, responsible, and ethical manner is fundamental to our daily operations.

DLD strives to protect and respect personal information of its client's employees and business partners and associates, in accordance with all applicable Provincial and Federal laws relating to privacy legislation including Personal Information and Electronics Protection and Documents Act (PIPEDA) and Personal Health Information Protection Act (PHIPA). Each staff member must abide by DLD's procedures and practices when handling private and confidential personal information.

Applicability

DLD is committed to protecting private personal information and has established methods to ensure privacy is maintained. This Privacy Policy applies to all personal information within DLD Group's possession and control.

Personal information is defined as any identifying information about an individual or group of individuals, including name, date of birth, address, phone number, e-mail address, social insurance/security number, nationality, gender, health history, financial data, credit card numbers, bank account numbers, assets, debts, liabilities, payment records, credit records, loan records, opinions, and personal views.

Business information is defined as business name, business address, business telephone number, name(s) of owner(s), executive officer(s), and director(s), job titles, business registration numbers, and financial status. Business information is treated and handled with the same level of confidentiality, privacy, and respect as personal information.

Appropriate Use

DLD collects and uses personal information solely for the purpose of conducting its business. Information obtained by DLD will never be shared with any individuals or outside organizations for any purpose other than those related to delivering services for clients.

Personal information will never be used for marketing promotional purposes. DLD will never sell or make available client personal information or business information to a third party.

Implementation Guidelines

1. DLD obtains personal information directly from the individual to which the information belongs. Individuals are entitled to know how DLD uses personal information and how DLD will limit the use of any personal information collected to what is needed for those stated purposes. DLD will obtain individual consent if personal information is to be used for any other purpose. DLD will not use any personal or business information without the consent of the client and/or affected individuals.

2. Under no circumstances will DLD sell, distribute, or otherwise disclose personal information or contact lists to third parties. However, limited disclosure may be required as part of DLD fulfilling its stated business duties and day-to-day operations. This may include consultants, suppliers, or business partners of DLD but only with the understanding that these parties obey and abide by this Privacy Policy, to the extent necessary of fulfilling their own business duties and day-to-day operations.

3. DLD vows to protect personal information with the appropriate security measures, physical safeguards, and electronic precautions. DLD maintains personal information through a combination of paper and electronic files. Where required by law or disaster recovery/business continuity policies, older paper records may be stored in a secure, offsite location. Back up electronic records are fully encrypted and are stored on a fully secured offsite locations.

4. Access to personal information will be authorized only for the employees and other agents of DLD Group Inc. who require the information to perform their job duties, and to those otherwise authorized by law.

5. DLD's computer and network systems are secured by complex security protocols and passwords. Only authorized individuals may access secure systems and databases.

6. Routers and servers connected to the Internet are protected by firewalls, and are further protected by virus attacks or "snooping" by anti-virus software solutions.

Software Development

1. The data centre of the software development site provides fully managed enterprise security that includes comprehensive web protection services, managed firewall, log monitoring, dual authentication, enforcement of change management protocols and real time event notifications. Network Service Gateways ensures the security scalability for data centre applications.

2. Servers are monitored through live sensor backups – constantly pinging the website to confirm that the systems are properly functioning. Feedback to on-call systems are administrated 24/7. Failover system is connected to offsite backup servers with a 15 second switching delay.

3. The overall security of the application(s) and data is addressed by the following means:
    a) Communication is secured via AES 128. Auto redirection to encrypted site ensures user cannot access non encrypted version of site.
    b) Logout after period of inactivity – set time by client.
    c) Application uses VPN for version control.
    d) Application code stored on web server is obfuscated to protect coding.
    e) Hosting software is continuously updated by the web hosting provider.
    f) Development site uses an intrusion prevention system with the sonic firewall.

4. The security architecture and cryptography used for each state, either at rest or in transmission, is detailed below:
    - Rest – Obfuscation of Code by deploying published dlls for back end code.
    - Transmitting AES 128 – SSL Certificate – Geo Trust Verifications.

5. Security certification and/or accreditation is achieved using SSAE 16 Type ll Certified and SSL Certification Authenticated through GEO Trust.
6. All software adheres to official internet protocols and standards with one (1) exception. Web server uses a proprietary protocol (1433) for the SQL port to lock it to our static IP which is then authenticated by a user name and password.

Privacy Breach Protocol

DLD has a privacy breach protocol that ensures immediate action is taken upon learning of a privacy breach. The following steps will be carried out simultaneously and in quick succession in the event of a privacy breach.

STEP 1: Immediately Implement Privacy Breach Protocol

a) DLD will notify all relevant staff and client of the breach, including the Chief Privacy Officer or *PHIPA* contact person, and determine who else from DLD should be involved in addressing the breach.

b) DLD will develop and execute a plan designed to contain the breach and notify those affected.

STEP 2: Stop And Contain The Breach

DLD will identify the scope of the breach and take the necessary steps to contain it, including:

a) Retrieving and securing any personal information that has been disclosed.

b) DLD will ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information.

c) Contact information will be obtained, in the event that follow-up is required.

d) DLD will determine whether the privacy breach would allow unauthorized access to any other personal information (e.g. an electronic information system) and take necessary steps, such as changing passwords, identification numbers and/or temporarily shutting your system down.

STEP 3: Notify Those Affected By The Breach

DLD will notify those individuals whose privacy was breached, including:

a) Identify all affected individuals and notify them of the breach at the first reasonable opportunity, via by telephone or in writing, depending on the circumstances.
b) When notifying individuals affected by a breach the following information will be provided:
    - Details of the breach to affected individuals, including the extent of the breach and what personal information was involved.
    - Steps taken by DLD to address the breach.
    - That they are entitled to make a complaint to the IPC.
    - Contact information for DLD staff who can provide additional information, assistance and answer questions.

STEP 4: Investigation and Remediation

a) DLD will conduct an internal investigation, including:

    - Ensure that the immediate requirements of containment and notification have been met.
    - Review the circumstances surrounding the breach.
    - Review the adequacy of existing policies and procedures in protecting personal information.

b) Ensure all staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of *PHIPA and PIPEDA*.

Policy Established: July 2014 Updated: August 2017