

Mailing Security Protocol

Locations:

2 Old Mill Road Caldwell NJ 07006
1140 Broadway New York NY 10003
1710 Dividend Road Ft Wayne IN 60608
14 Henderson Drive West Caldwell NJ 07006

Please find a Summary of Directed Online privacy policy and procedures for handling of confidential information. This has been in place since 2007 when Directed was formed.

- Since its inception, DIRECTED ONLINE has been constructed around the handling and producing of highly sensitive data for our clients. Our facility is perimeter secured. Every visitor must provide identification and sign in. Suppliers are not permitted beyond the front office area. All areas are hand scan access (biometric) controlled and all cameras are digitally managed and provide facial recognition. Cameras are monitored and security personnel guard the property 24 hours per day.
- Directed Online facilities and processes are audited no less than two times yearly by the Infosec and Security departments of two of the world's leading financial institutions. These teams evaluate physical and electronic security and require adherence to the same standard as their facilities and processes. DIRECTED ONLINE has never failed one of these audits.
- Employees: Every employee of DIRECTED ONLINE worldwide is subjected to a criminal background check that is at least as stringent as the standard of Directed Online investment banking and financial services clients.
- Data security: All data is housed behind firewalls. All DIRECTED ONLINE data networks are penetration tested on a regular basis. In the course of conducting our business and providing services, DIRECTED ONLINE receives, maintains, processes, and transmits large amounts of DIRECTED ONLINE and client confidential information. DIRECTED ONLINE is firmly obligated and committed to protect the confidentiality of this information.
- Internal: All client data is considered confidential. All physical and electronic access to IT systems, networks, and confidential information, is limited to DIRECTED ONLINE associates with a business need.
- Internal network access to DIRECTED ONLINE and client data is gated by USER ID/Password authentication. Typically, dual perimeter User ID authentication is the rule. All password protection includes lockouts, minimum lengths, and alphanumeric composition and where applicable two-factor authentication techniques.
- Client Data is not used for development, testing, training, or any purpose other than providing production service, client specific acceptance testing, or production diagnostics.
- Actual or requested document archiving is conducted in accordance with the DIRECTED ONLINE Record Retention Policy.
- All physical and electronic access is immediately reviewed upon any change in job assignment and all access is terminated immediately leaving DIRECTED ONLINE employment.
- External: External transmission of client data is conducted utilizing approved secure methods. Such methods include, but not limited to, Secure FTP, PGP/FTP HTTPS, Secure NDM, dedicated point to point data lines, etc. All encryption algorithms, modes of operation, and security key management systems are consistent with internal standards issued by the Corporate Security Group.
- Web-Based products and platforms are domain name registered (with the domain name registration authority) and where applicable utilize approved data transmission methods (SSL, IPsec, HTTPS, etc.) Appropriate security measures are used to protect Directed Online infrastructure, including using firewalls and perimeter LAN/WAN infrastructures to control Internet access to the appropriate web and/or back-end devices. These same products and platforms undergo attack and penetration testing before becoming operational and periodically thereafter.

Cont'd...

Area of Focus	DIRECTED ONLINE Approach
Audit Trail	We receive encrypted files via our Secure FTP site or PGP encryption. This is logged on our servers that collect files. From there, files are locked down via Active Directory permissions and a disclaimer is presented upon logging into these systems.
Archiving, Purging Intervals	The data archiving and purging differs as it is an agreement made with each customer.
Data Transfer Options	Email, FTP, HTTPS, WAMNET, Virtual Private Network, Point to Point
Disposal of Data and Materials	Hard disks are magnetically erased, disassembled, and then destroyed. CD's and tapes are destroyed. In some cases, with customer data, we use one of our vendors to properly destroy and dispose of customer data, using DOD scrub with written evidence. All physical waste is automatically shredded and recycles via automatic waste retrieval systems. All excess materials at the completion of project are shredded within facilities. Secure shredding is provided for all materials containing PII or data classified as highly sensitive within controlled production environment.
Technology Perimeter Defense:	Best in Class Firewalls and IDS. Routers with ACL's.
Data Retention	Logs are kept in our Syslog server for 6 months and they are unalterable.
Securing Backups	Backups are written to tape and off-sited by our Disaster Recovery and Storage Vendor "GRM" – Guarantee Records Management Corp.
Employee back-ground checks performed:	Every employee of DIRECTED ONLINE is subjected to a criminal background check that is at least as stringent as the standard of Directed Online investment banking and financial services clients.
	As part of the DIRECTED ONLINE North Pre-employment Procedures, all new hired employees are required to sign a release authorization authorizing DIRECTED ONLINE in North America to run an investigative consumer report. The employee is also given a written summary of their rights under the Fair Credit Reporting Act. The following items are requested on all background checks:
	· Verification of Address
	· Verification of Social Security #
	· Verification of past or present education
	· Verification of Criminal background (Nationwide)
	· Verification of name
	· Verification of past credit
	Once the authorization is received from the employee, we electronically process the request and receive the detailed report within 15 minutes to 1 hour depending on the extent of the background history.

Cont'd...

Data safeguard	On systems that contain customer data, the security is locked down via Active Directory permissions, which is reviewed regularly, and a disclaimer is presented upon logging into these systems.
File Transfer Protocol (ftp) site specification	We use SSL 128-bit encryption on our FTP server and transmission.
Preferred encryption protocols	PGP and 128-bit SSL
What procedures are in place for setting, controlling, and modifying vendor access?	We have standards according to our DIRECTED ONLINE Information Security Policy that is reviewed regularly. These procedures are also audited by an outside audit firm, Grant Thornton, as well as approved and managed by our InfoSec team.
Environmental controls	Alarming is currently setup and auto-notifications are sent to our team.
Are procedures in place for notification and escalation in the event of a security incident?	Alarming is currently setup and auto-notifications are sent to our team.
Perimeter defense devices configured for least access	Implicit denies are on all firewall rule bases and ACL's
Network devices and critical hosts monitoring	We use Juniper SSG520's for IDS with alarming and notifications to our Management Console.
Anti-virus software	Sophos Enterprise Anti-virus is installed and configured. All updates are pushed hourly.
Multi-factor authentication (e.g. RSA Tokens)	We use RSA 2-factor tokens for outside VPN access. This access is only granted to employees with restricted access. We also use MD5 encryption on the VPN tunnels.
Penetration testing	We use accredited third-party firms for regular penetration tests.
SOC Audits	Our systems and facilities are subjected to SOC audits annually by an accredited third part firm.

Cont'd...

Data Handling and Privacy Agreement

1. Confidentiality and Data Protection

1. DIRECTED ONLINE and its DIRECTED ONLINE Personnel will treat as confidential all information and data, of whatever nature, relating to our clients (including but not limited to information and data regarding our clients operations, research, policies, procedures, data, techniques, accounts and its personnel) or used by our clients or any of our client's personnel in carrying on business, which is obtained or accessed by DIRECTED ONLINE or its DIRECTED ONLINE Personnel, or disclosed to DIRECTED ONLINE or its DIRECTED ONLINE Personnel in connection with the performance by DIRECTED ONLINE of Directed Online obligations under an agreement; (c) all information and data which are proprietary to a third party (including but not limited to our client's customers and suppliers) and which our clients is obligated to treat as confidential, obtained by DIRECTED ONLINE or its DIRECTED ONLINE Personnel, or disclosed to DIRECTED ONLINE or its DIRECTED ONLINE Personnel in connection with the performance by DIRECTED ONLINE of Directed Online obligations under an agreement; and (d) Customer Information (individually and collectively, "Confidential Information"). **"Customer Information"** means all information, in any form (e.g., written, verbal, electronic), provided to, or collected or generated by, the DIRECTED ONLINE or to which the DIRECTED ONLINE or its DIRECTED ONLINE Personnel have been given access by or on behalf of our clients, that uniquely identifies a current, former or prospective our clients customer or customer of any correspondent bank or customer financial institution and includes, but is not limited to, Personal Information. Customer Information further includes, but is not limited to, whole or partial copies of such information or materials derived from such information. DIRECTED ONLINE shall immediately by phone and promptly in writing (but in no event more than twenty-four (24) hours of discovery), notify our clients if it becomes aware of: (i) any loss of Customer Information; (ii) any attempt to obtain unauthorized access to, disclosure of or use of Customer Information; or (iii) any attempt to alter or destroy Customer Information and, in such event, at no additional cost to our clients shall cooperate fully with our clients and follow our client's instructions regarding actions to be undertaken to address such loss or breach.

2. DIRECTED ONLINE and its DIRECTED ONLINE Personnel shall not disclose, use, publish or otherwise reveal, directly or indirectly through any third party, any Confidential Information (including without limitation Personal Information) to any third person or to any of Directed Online DIRECTED ONLINE Personnel that do not have a need to know such Confidential Information for the purpose of their role in performing Directed Online obligations under an agreement. DIRECTED ONLINE shall exercise the same degree of care to keep confidential any Confidential Information disclosed to DIRECTED ONLINE as DIRECTED ONLINE exercises to keep confidential its own information of like nature, but in no event less than a reasonable standard of care. DIRECTED ONLINE will instruct its DIRECTED ONLINE Personnel to comply with their individual obligations as well as Directed Online obligations set forth in this Section 11, and DIRECTED ONLINE will obtain a signed agreement substantially in the form of Exhibit B hereto from any DIRECTED ONLINE Personnel performing Services or with access to Customer Information.

3. DIRECTED ONLINE and its DIRECTED ONLINE Personnel shall not use any Confidential Information to obtain an unauthorized benefit for DIRECTED ONLINE, our clients or any third party.

4. Notwithstanding the foregoing, for Confidential Information that is not Customer Information, the above restrictions on disclosure shall not apply solely with respect to information and material that: (i) is received from any third party source that is properly authorized to disclose it without restriction on such disclosure; (ii) is or becomes generally known to the public by publication or other means other than a breach of duty under an agreement or any other agreement by DIRECTED ONLINE or any of its DIRECTED ONLINE Personnel; or (iii) is required by law, regulation or court order to be divulged, provided that the request for such disclosure is proper and the disclosure does not exceed that which is required. In no event shall Customer Information be subject to the preceding exceptions. In the event of any disclosure under (iii) above, a copy of this agreement shall be furnished to anyone to whom such disclosure is required, and the disclosing party shall promptly, prior to disclosure, advise the other party in writing of each such disclosure and, at the other party's cost, shall reasonably cooperate with the other party to prevent or limit such disclosure as permitted by law.

Cont'd...

5. DIRECTED ONLINE hereby acknowledges that enforcement of this agreement through claims for damages would be inadequate and that, in the event of a breach or threatened breach of this Section 11, our clients

shall be entitled to any necessary judicial relief, including without limitation injunctive relief, without the necessity of having to post a bond.

6. Upon our clients' request, and in any event upon termination of an agreement, DIRECTED ONLINE shall return the original and any copies of the Confidential Information which it, or any of its DIRECTED ONLINE Personnel are holding in tangible form, written or otherwise, to our clients or, at our clients' option, shall destroy such information and shall certify in writing to our clients that such Confidential Information has been destroyed.

7. DIRECTED ONLINE will comply with data privacy laws in relation to the processing of personal data in connection with an agreement. DIRECTED ONLINE will not, by any act or omission, place any member of our client's group in breach of the data privacy laws. For the purpose of an agreement "data privacy laws" means all relevant provisions of the worldwide directives and any other relevant and applicable data protection legislation, guidelines and industry standards (to the extent applicable) in the jurisdictions from which and to which the relevant Services are to be performed.

8. DIRECTED ONLINE will comply with, and only act on, instructions from and on behalf of the relevant member of our client regarding the processing of our clients Personal Data and DIRECTED ONLINE will not process the our clients Personal Data for any purposes other than to provide the Services to the relevant member of the our clients Group. For the purpose of an agreement "our clients Personal Data" means any personal data supplied by any our clients Group Member or on its behalf to Supplier and/or processed in connection with an agreement.

9. DIRECTED ONLINE will ensure that appropriate technical and organizational measures are taken to avoid unauthorized or unlawful processing of our clients Personal Data and against loss or destruction of or damage to our clients Personal Data. DIRECTED ONLINE must ensure that the technical and organizational measures it implements ensures a strict separation between our clients Personal Data, and other personal data in respect of which DIRECTED ONLINE is a data controller or a data processor.

10. DIRECTED ONLINE will inform the relevant member of our clients immediately of any suspected or confirmed data protection breaches, unauthorized or unlawful processing, loss, or destruction of, or damage to, our clients Personal Data.

11. DIRECTED ONLINE will comply with any reasonable request made by our clients to ensure compliance with the measures set out in this agreement.

12. DIRECTED ONLINE will take reasonable steps to ensure the reliability of its DIRECTED ONLINE Personnel who obtain access to our clients Personal Data pursuant to, or in connection with, the provision of the Services.

13. DIRECTED ONLINE will ensure that its DIRECTED ONLINE Personnel are suitably informed, trained and instructed in respect of data privacy laws as well as obliged to observe data secrecy regulations pursuant to the relevant applicable data protection laws. DIRECTED ONLINE will procure that its Personnel observe any applicable data secrecy regulations beyond their respective periods of employment with DIRECTED ONLINE.

DIRECTED ONLINE will not, unless requested by our clients or obliged by law, disclose our clients Personal Data to any third party. If DIRECTED ONLINE is obliged by law to disclose our clients Personal Data to any third party, DIRECTED ONLINE will (to the extent permitted by law) inform our clients of such intended disclosure and co-operate with our clients to limit the scope of the disclosure to what is strictly required by law.