



INFORMATION SECURITY & PRIVACY INSURANCE WITH ELECTRONIC MEDIA LIABILITY COVERAGE

NOTICE: COVERAGE UNDER THIS POLICY IS PROVIDED ON A CLAIMS MADE AND REPORTED BASIS AND APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENSION PERIOD (IF APPLICABLE) AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD OR AS OTHERWISE PROVIDED IN CLAUSE X. OF THIS POLICY. AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO RETENTIONS.

PLEASE READ THIS POLICY CAREFULLY.

Please fully answer all questions and submit all requested information. If the Applicant is a private company, please attach a copy of your most recent financial statement.

I. GENERAL INFORMATION			
Full Name:	HIDALGO COUNTY		
Mailing Address:	9805 N. 10 th St.	State of Incorporation:	TEXAS
City:	McALLEN	State & Zip:	TX 78504
# of Employees:	3545	Date Established:	1852
Website URL's:	WWW.CO.HIDALGO.TX.US		
Authorized Officer ¹ :	VALDE GUERRA	Telephone:	(956) 292-7655
		E-mail:	VALDE.GUERRA@CO.HIDALGO.TX.US
Business Description:	COUNTY GOVERNMENT		

II. REVENUE INFORMATION:			
	Most Recent Twelve (12) months: (ending: 12/31/13)	Previous Year	Next Year (estimate)
US Revenue:	174,330,471.00	165,648,723.00	175,000,000.00
Non-US Revenue:			
Total Revenue:	174,330,471.00	165,648,723.00	175,000,000.00

Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes in the past twelve (12) months? Yes No

If yes, please explain:

Has the Applicant in the past twelve (12) months completed or agreed to, or does it contemplate within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed? Yes No

If yes, please explain:

¹ The officer of the Applicant that is designated to receive any and all notices from the Insurer or its authorized representative(s) concerning this insurance.

III. MANAGEMENT OF PRIVACY EXPOSURES		
1. Has the Applicant designated a Chief Privacy Officer? If no, please indicate what position (if any) is responsible for privacy issues:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
2. Does the Applicant have a written corporate-wide privacy policy? If yes, please attach a copy of the privacy policy to this application.	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
3. Is the Applicant in compliance with its privacy policy? If no, please provide details regarding such non-compliance:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
4. Does the Applicant accept credit cards for goods sold or services rendered? If yes: A. Please state the Applicant's approximate percentage of revenues from credit card transactions in the most recent twelve (12) months: B. Is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)? If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
5. Does the Applicant restrict employee access to personally identifiable on a business-need to know basis?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does the Applicant require third parties with which it shares personally identifiable information or confidential information to indemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
7. Is the Applicant aware of any release, loss or disclosure of personally identifiable information in its care, custody or control, or anyone holding such information on behalf of the Applicant in the most recent three year time period from the date of this Application? If yes, please describe:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
8. Has the Applicant implemented an identity theft prevention program (aka FTC "Red Flags" program)?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

SEE ATTACHED

% 2.1

IV. COMPUTER SYSTEMS CONTROLS <i>If the Applicant has completed a full IT-Security Assessment, please check here <input type="checkbox"/> and skip this section.</i>					
1. Has the Applicant designated a Chief Security Officer as respects computer systems? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If no, please indicate what position is responsible for computer security:					
2. Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No					
3. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its computer systems? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No					
4. Does the Applicant have : A. a disaster recovery plan? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No B. a business continuity plan? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No C. an incident response plan for network intrusions and virus incidents? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No How often are such plans tested? <u>YEARLY</u>					
5. Does the Applicant have a program in place to test or audit security controls on an annual or more frequent basis? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If yes, please summarize the scope of such audits and/or tests: <u>AUDIT DONE QUARTERLY (SECURITY ASSESSMENT OF NETWORK)</u>					
6. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No					
7. Is all valuable/sensitive data backed-up by the Applicant on a daily basis? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If no, please describe exceptions:					
8. Is at least one complete back-up file generation stored and secured off-site separate from the Applicant's main operations in a restricted area? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If no, describe the procedure used by the Applicant, if any, to store or secure copies of valuable/sensitive data off-site?					
9. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No A. Does the Applicant encrypt data stored on laptop computers and portable media? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No B. Does the Applicant encrypt data stored on back-up tapes? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No C. Does the Applicant encrypt data "at rest" within computer databases? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No					
10. Does the Applicant enforce a software update process including installation of software "patches"? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If Yes, are critical patches installed within thirty (30) days of release? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No					
11. Please describe your network infrastructure:					
	Anti-virus	Firewall	ISP	Intrusion Detection	
Primary vendor:	<u>TREND MICRO</u>	<u>CISCO</u>	<u>TIME WARNER</u>	<u>CISCO</u>	
Other significant vendor:					
12. How often are virus signatures updated? <input checked="" type="checkbox"/> Automatic Updates <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly <input type="checkbox"/> Other					

13. Does the Applicant require computer service providers who may have access to confidential information or personally identifiable information to demonstrate adequate security policies and procedures?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
A. Are computer service providers required by contract to indemnify the Applicant for harm arising from a breach of the provider's security?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
14. Has the Applicant suffered any known intrusions (i.e., unauthorized access or security breach) or denial of service attacks relating to its computer systems in the most recent three (3) year time period from the date of this Application? If yes, describe any such intrusions or attacks, including any damage caused by any such intrusions, including lost time, lost business income, or costs to repair any damage to systems or to reconstruct data or software, describe the damage that occurred, and state value of any lost time, income and the costs of any repair or reconstruction:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

SEE ATTACHED MEMO DATED JUNE 1, 2014

V. CONTENT CONTROLS		
1. Please describe content produced by the Applicant:	DATA & SERVICES (BOTH PUBLIC & CONFIDENTIAL)	
2. Does the Applicant have a procedure for responding to allegations that content created, displayed or published by the Applicant is libelous, infringing, or in violation of a third party's privacy rights?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
3. Does the Applicant have a qualified attorney review all content prior to posting on the Insured's Internet Site? If yes, does the review include screening the content for the following:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
A. disparagement issues?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
B. copywriting infringement?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
C. trademark infringement?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
D. invasion of privacy?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
If no to question 3., please describe procedures to avoid the posting of improper or infringing content:		
4. Has the Applicant screened all trademarks used by the Applicant for infringement with existing trademarks prior to first use?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
A. Has the Applicant acquired any trademarks from others in the past three (3) years?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
If Yes, were acquired trademarks screened for infringement?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
5. Within the last three (3) years, has the Applicant ever received a complaint or cease and desist demand alleging trademark, copyright, invasion of privacy, or defamation with regard to any content published, displayed or distributed by or on behalf of the Applicant?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
If yes, please provide details regarding any such demands:		

VI. PRIOR INSURANCE					
1. Does the Applicant currently have insurance in place covering media, privacy or network security exposures?					
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No					
If yes, please provide the following:					
Insurer N/A	Limits	Retention	Policy Period	Premium	Retroactive Date

N/A					
-----	--	--	--	--	--

2. Has any professional liability, privacy, network security or media insurance ever been declined or cancelled? If yes, please provide details:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
---	------------------------------	--

VII. PRIOR CLAIMS AND CIRCUMSTANCES		
1. Has the Applicant ever received any claims or complaints with respect to allegations of invasion of or injury to privacy, identity theft, theft of information, breach of information security, software copyright infringement or content infringement or been required to provide notification to individuals due to an actual or suspected disclosure of personal information? If yes, Provide details of each such claim, allegation or incident, including costs, losses or damages incurred or paid, and any amounts paid as a loss under any insurance policy:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
2. Has the Applicant been subject to any government action, investigation or subpoena regarding any alleged violation of any law or regulation? If yes, please provide details of any such action, investigation or subpoena:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
3. Has the Applicant ever experienced an extortion attempt or demand with respect to its computer systems? If yes, please provide details:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
4. Has the Applicant notified consumers of a data breach incident in accordance with a data breach notification law in the past three (3) years? If yes, please provide details:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
5. Has the Applicant notified consumers of a data breach incident in accordance with a data breach notification law in the past three (3) years? If yes, please provide details:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
6. Does the Applicant, or any director, officer, employee or other proposed insured have knowledge or information of any fact, circumstance, situation, event or transaction which may give rise to a claim or privacy breach notification under the proposed insurance? If yes, provide details:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

THE UNDERSIGNED IS AUTHORIZED BY THE APPLICANT AND DECLARES THAT THE STATEMENTS SET FORTH HEREIN AND ALL WRITTEN STATEMENTS AND MATERIALS FURNISHED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION ARE TRUE. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THE STATEMENTS CONTAINED IN THIS APPLICATION, ANY SUPPLEMENTAL APPLICATIONS, AND THE MATERIALS SUBMITTED HERewith ARE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED AND HAVE BEEN RELIED UPON BY THE INSURER IN ISSUING ANY POLICY.

THIS APPLICATION AND MATERIALS SUBMITTED WITH IT SHALL BE RETAINED ON FILE WITH THE INSURER AND SHALL BE DEEMED ATTACHED TO AND BECOME PART OF THE POLICY IF ISSUED. THE INSURER IS AUTHORIZED TO MAKE ANY INVESTIGATION AND INQUIRY IN CONNECTION WITH THIS APPLICATION AS IT DEEMS NECESSARY.

THE APPLICANT AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, THE APPLICANT WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.



I HAVE READ THE FOREGOING APPLICATION FOR INSURANCE INCLUDING ATTACHMENT 'A' AND REPRESENT THAT THE RESPONSES PROVIDED ON BEHALF OF THE APPLICANT ARE TRUE AND CORRECT.

FRAUD WARNING

ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT (S)HE IS FACILITATING A FRAUD AGAINST AN INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT MAY BE GUILTY OF INSURANCE FRAUD.

NOTICE TO COLORADO INSURED: IT IS UNLAWFUL TO KNOWINGLY PROVIDE FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES, DENIAL OF INSURANCE, AND CIVIL DAMAGES. ANY INSURANCE COMPANY OR AGENT OF AN INSURANCE COMPANY WHO KNOWINGLY PROVIDES FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO A POLICYHOLDER OR CLAIMANT FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE POLICYHOLDER OR CLAIMANT WITH REGARD TO A SETTLEMENT OR AWARD PAYABLE FROM INSURANCE PROCEEDS SHALL BE REPORTED TO THE COLORADO DIVISION OF INSURANCE WITHIN THE DEPARTMENT OF REGULATORY AGENCIES.

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: WARNING: IT IS A CRIME TO PROVIDE FALSE OR MISLEADING INFORMATION TO AN INSURER FOR THE PURPOSE OF DEFRAUDING THE INSURERS OR ANY OTHER PERSON. PENALTIES INCLUDE IMPRISONMENT AND/OR FINES. IN ADDITION, AN INSURER MAY DENY INSURANCE BENEFITS IF FALSE INFORMATION MATERIALLY RELATED TO A CLAIM WAS PROVIDED BY THE APPLICANT.

NOTICE TO FLORIDA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO INJURE, DEFRAUD, OR DECEIVE ANY INSURER FILES A STATEMENT OF CLAIM OR AN **APPLICATION** CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY IN THE THIRD DEGREE.

NOTICE TO LOUISIANA AND MARYLAND APPLICANTS: ANY PERSON WHO KNOWINGLY AND WILLFULLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR WHO KNOWINGLY AND WILLFULLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

NOTICE TO MINNESOTA APPLICANTS: A PERSON WHO FILES A CLAIM WITH INTENT TO DEFRAUD OR HELPS COMMIT A FRAUD AGAINST AN INSURER IS GUILTY OF A CRIME.

NOTICE TO MAINE, TENNESSEE, VIRGINIA AND WASHINGTON APPLICANTS: IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.

NOTICE TO OKLAHOMA APPLICANTS: ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY.

NOTICE TO PENNSYLVANIA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN **APPLICATION**



FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME AND SUBJECTS SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

NOTICE TO NEW YORK APPLICANTS AND KENTUCKY: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN **APPLICATION** FOR INSURANCE OR STATEMENT OF CLAIMS CONTAINING ANY MATERIALLY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME, AND NEW YORK APPLICANTS SHALL ALSO BE SUBJECT TO A CIVIL PENALTY NOT TO EXCEED FIVE THOUSAND DOLLARS AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.

Signed:

Must be signed by corporate officer with authority to sign on Applicant's behalf

Date: ____ ____ ____
 Day Month Year

Information Technology (IT) Security Policies - Section 2 - Policy Standards	03/2004 – Effective 01/27/2014 – Revised By: Renán Ramirez
--	--

Policy 10.00 – Information Technology Privacy Policy

- ALL Electronic media (analog and digital; video, files or other media) created, sent, received, recorded or otherwise stored on information resources owned, leased, administered, or otherwise under the custody and control of Hidalgo County are not private and may be accessed by Hidalgo County at any time without knowledge of the IR user or owner.
- Electronic media controlled by Law Enforcement may, in certain cases, be deemed evidence and not subject to access by non law enforcement staff.
- To manage systems and enforce security, Hidalgo County may log, review, and otherwise utilize any information stored on or passing through its IR systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these same purposes, Hidalgo County may also capture User activity such as telephone numbers dialed and web sites visited.
- A wide variety of third parties have entrusted their information to Hidalgo County for business purposes, and all workers at Hidalgo County must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.
- Users must report any weaknesses in Hidalgo County computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access or install any data or programs contained on Hidalgo County systems for which they do not have authorization or explicit consent from the department system administrator or the IT department.

COUNTY of HIDALGO, Texas

Information Technology Department

100 N. Closner Blvd.
Edinburg, TX 78539
956-292-7010
www.co.hidalgo.tx.us



June 1, 2014

MEMORANDUM

As per your request, the following is a brief description of the events of April 25, 2014. Since the incident is still under investigation by law enforcement agencies, I am not allowed to share specific details.

On the night of April 25, 2014, a person outside the County logged into our County email system. Our log files show this person logged in around 9:45PM. At 10:14PM an email was sent to all users of the email system with vulgar language and technical references to vulnerabilities of the operating system that is run on the County mail server. Fortunately we became aware immediately of this email and shut down the County's mail server within ten minutes of the receipt of this email.

Over the weekend the County's Information Technology staff worked to check the security of the entire county network. Configurations and passwords were changed, log files were reviewed, and outside security experts were brought in to look at our network. Since that time the Information Technology department has further enhanced the security of the County's information system resources, implemented tighter security policies for users and will purchase advanced network security devices and services.

We are confident that no County data was compromised or lost. We will continue to enhance our security and internal procedures in order to mitigate any future risks.

I thank you for your time and attention to this matter, if you have any questions feel free to contact me.

Renan A. Ramirez
Chief Information Officer
Hidalgo County, Texas

QUESTION 14 SUPPLEMENT