/ IT SECURITY POLICY

CONTENTS

ICOVER channels all requests through our in-house screening platform

The Global Verifications software platform resides in SAS70 compliant data centre. Once a user logs in to global verifications, all communication is secured via SSL. SSL, Short for Secure Sockets Layer, is a protocol developed for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.

HOW WE OVERCOME THE MOST COMMON WEB SECURITY CHALLENGES?

SQL injection

Global Verifications uses Oracle's MySQL database and the Hibernate persistence layer, which automatically escapes SQL queries when committing to database to prevent SQL Injection attacks.

XSS - cross-site scripting injection

The Global Verifications platform ensures that all data values rendered into views are escaped correctly.

In addition, it avoids the use of request parameters or data fields for determining the next URL to redirect the user to.

DOS – Denial of Service Attack

We have a DOS protection in front of the primary production servers which is scanning the traffic and making sure that DOS attack is not reaching our production instances.

Cross-Site Request Forgery

We have a system in place to protect our system from attackers trying to trick users from performing actions without their knowledge.

Preventing Sensitive Data Exposure

We have an encrypted highly secured connection between internal database instance which keeps the data highly secured without any “data bleeding”.

Security Misconfiguration

The company has in place a high level of Software Firewall protection combined with a Hardware such on the front of the server before the access requests reach the application which means that all the traffic is filtered in advance.

How we ensure Data Protection?

There are processes in place for data protection and available disaster recovery plan in place which includes a highly secured data centre accessed only by certified staff.

We also maintain an additional security level of verification for getting access to each data centre branch which guarantees no data access from external individuals or companies.

1. MANAGING IT INTERRUPTIONS

- IT interruptions or data loss recovery plans are of great importance to ICOVER because they directly impact our clients and could result in potential loss of revenue for our clients. The following is an outline of ICOVER'Ss backup procedures and disaster recovery plan should a major outage occur.
- ICOVER IT department performs each business day a comprehensive backup of all data bases,
- Tables, data files and image files on a 45-business day rotation.
- The company has a real time syncing system in place which allows to make a real time back up of any data coming into the system through a RAID connection to other Hard Drives which guarantees a 100% data safety
- The company also has a system which allows an immediate replacement of Hard Drives in case of failure without any data loss during the work with the system.
- The whole infrastructure works with a set of back up servers which can be turned on automatically in a case of failure of the primary ones
- Databases are using replications which allow easy and fast switch from one server to another in a case of failure
- Physical files are backed up with incremental technology which allows restoring from any point of failure

2. INCIDENT RESPONSE PROCEDURES

Our resolution policy consists of taking immediate steps to stop the breach and to ensure that no further breach can occur. Our Quality Manager has immediate authority to direct all and any resources to ensure that client's data is protected.

Contact is made with the Client to inform them of the situation and to advice on the following:

- What steps ICOVER has completed to minimize the exposure of data.
- What steps ICOVER will do to minimize damage from the breach.
- What steps ICOVER will do to prevent another similar event from happening.

We will coordinate between the client and the involved office to ensure that the matter is resolved as soon as possible. Pre-Employment Screening director will oversee all areas including disciplinary action to those responsible for the breach.

Data loss: our Data Breach – Includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access, to data, whether physical or electronic.

3. OUR NETWORK FRAMEWORK AND ITS SECURITY MAINTENANCE

- ICOVER'S operational environment is based on Linux /Ubuntu/ and Intel platform. ICOVER'S in-house and web applications are multi-tier apps with HTML5 / Vue JS front-end, server middle tier, and MySQL/MongoDB database backend.
- ICOVER employs Microsoft Active Directory service to provide central control and central administration to ICOVER'S applications, network resource, and users.
- All ICOVER workstations are joined to ICOVER domain. Multiple domain controllers are deployed across ICOVER'S enterprise network to provide efficient and timely access, as well as system redundancy.
- Each user is assigned to specific Active Directory groups according to user's job functions. Each Active Directory group is associated with its own access rules and security
  policies. When logging on, the user is authenticated by Active Directory. Once logged on, the user can only access pre-defined applications and network resources assigned to that user.
- Users do not have direct access to data. Applications retrieve data from business logic middle tier. ICOVER applications are accessible only by authorized user after user is authenticated by the applications
- Customer data is logically separated through the following implementation of a Virtual Private Database.

3.1. DEFINED USER ROLES

- The database defines user roles that control how end users (Internal & external) will access data and objects stored within the database.
- End users both internal and external do not have direct access to the SQL Server database. Data is retrieved and submitted via Business Layer residing in an Application Server. Therefore, only the Application Server processes are granted a SQL queries and access.
- Only the Application Servers accounts and DBA accounts are allowed to make connections to the Database Server.
- Every Stored procedure, whether it is one that is designed to retrieve data or modify data, requires a session ID parameter built with a special salt key. This parameter allows the Stored Procedure to create a security context that is valid only for the duration of the call.
- A Session ID is obtained by providing a User ID and Password and optionally a Client Certificate. For external users this information is transmitted via SSL to our Web Servers and then forwarded via SSL to our Application Servers for Authentication. For internal users this information is transmitted directly to our Application Servers.
- A Session ID is set to expire after 60 minutes of inactivity.
- Each and every request for data must provide a valid session ID that is used to create a new security context at the beginning of the request. This security context is valid for only that request and is destroyed at the end of the request.
- Before any Stored procedure retrieves or modifies any data, the security context is interrogated to ensure that the associated session is valid and has not expired, that the associated user is valid and active and is authorized (Depending on his User Right

Management System for this Procedure i.e.. Read, Update and Delete) to execute part or all of this procedure and that this user's Client Control List (CCL) allows access to the information that he wants to retrieve or modify.

- A Client Identifier, that is an attribute of every row in the transactional tables, is used to segregate Clients data within our database. A user is granted access to one or more of these rows by comparing that row's Client Identifier to the users CCL.
- A packet filtering, IP forwarding Firewall with NAT enabled is used to isolate and protect ICOVER'S Web Server from public network. The Firewall integrates a powerful combination of dynamic state full packet firewall, VPN, Intelligent Layered Security (ILS) for Zero Day protection, gateway antivirus, intrusion prevention, anti-spy ware, URL filtering, and spam blocking.

3.2. ISSUING OF USER IDS, PASSWORDS AND CERTIFICATES FOR REMOTE INTERNET USERS

- ICOVER has an obligation to each client to maintain the integrity and security of their data and thus it is ICOVER'S responsibility to maintain and control who has access to our client data.
- We go to great lengths from a systems point of view to make sure of the integrity of the databases and image bases are maintained to the highest degree of security. However, we must make sure that when we do allow access to users outside of our own company, that we take the necessary precautions to ensure we have the authority from our clients to assign user names and passwords backed up by signed documentation from our clients.
- Specific procedures are implemented whenever assigning user ids and passwords as well as where security certificates are required.
- E-mail correspondence with clients may be used for non-sensitive information such as sending blank forms etc. Under no circumstances should user ids or passwords or certificate validation id's be delivered by e-mail.
- Before any access is given to any users, the client must complete in full the Internet Access Authorization Form. The form must be signed and returned to ICOVER. This form will be used to authenticate requests from the client for user id, passwords and certificates as needed by the client from time to time. This form should be put in a PDF file format and stored for easy access by the security administrator. The original documents must be filed in a locked cabinet.
- Before a user id, password or certificate is issued, an Internet User Access Request Form must be completed by the client and signed by the user and either the primary or secondary contact person that appears on the Internet Access Authorization Form.
- On receipt of a completed and signed Internet User Access Request Form, the security administrator must verify the request has been signed by either the primary or secondary contact. If so, then a user id, password and certificate if requested may be issued.
- If the security administrator is contacted by a user, who is requesting a new password or needs to revalidate a user id or password, or any information which would be in violation of our security policy, the security administrator will advise the caller to contact either the primary or secondary contact for their company.
- If for any reason the security administrator receives a request for user id, password or a certificate that does not have the correct primary or secondary contact on the request, then the request must be sent back to the attention of either the primary or

secondary contact indicating that we cannot process this request without appropriate proper authorization.

3.3. SYSTEM USERS AND PASSWORD RULES

- Enforce password history: last 10 passwords remembered
- Maximum password age: 90 days
- Minimum password age: 1 day
- Minimum password length: 8 characters
- Password must contain mixed case characters, numerals or punctuation and cannot contain your first or last name
- Passwords are stored using a one-way hash with a salt key
- Accounts are locked out after 5 invalid logon attempts
- Once an account is locked out, it remains locked for 60 minutes
- On all new accounts, passwords must be changed before first logon
- After a password reset, the password must be changed before the next logon
- Typical user id rollout, reset and change processes are described in the following section.

3.4. OUR INTERNET-BASED SERVICES

- ICOVER offers a fully secure web-based system that allows the Human Resources Representative to confidently submit requests for reports, view real time status notes on ongoing files and retrieve completed reports.
- The system is secured by SHA2 and 2048-bit SSL encryption which allows for the secure transaction of data between the client and ICOVER.
- All the data is encrypted before storing into the database and there is no direct access without decrypting it directly through the system with the specific customer account
- While a Human Resources Representative who has a user name and password can transmit information to ICOVER from any computer, the viewing of information and retrieval of reports could only be allowed by specific computers identified by the client. This is completed through certificate level security. This secure and user-friendly system controls the unauthorized access to information of a confidential/personal nature.
- We have a full-time support person who is available to assist the client in managing their web based needs. This includes setting up user IDs, passwords and adding certificates for retrieval purposes.

3.5. INTERNET SECURITY

- ICOVER website is hosted and secured by OVH (a French company). When you log into ICOVER website (using a pre-arranged confidential User ID and Password), you enter our secured area. This area is protected by Secure Sockets Layer (SSL) Protocol with 2048-bit encryption. This means that the information sent between your computer and our secure servers are encrypted while it is in transit. Unauthorized individuals on the Internet cannot view the information.

The Authentication Mechanism consists of challenging a user for his credentials (User ID/Password). This is then validated against the ICOVER External User Directory Server. The certificate's serial number is also validated along with the certificate's revocation status, expiry date and issuing authority. The transmission of the credentials is all done over 2048 bit SSL.

4. ESTABLISHED ISSUE LEVELS & RESOLUTION PROCESSES

ISSUE LEVEL 1, MINOR ISSUES RELATING TO:

- Time Service (less than 2 days)
- Incomplete Reports
- Spelling/Grammatical mistakes

Resolution Processes: Level 1 issues are immediately brought to the attention of the Supervisor and Office Manager. They are resolved quickly between the supervisor, investigator and the client directly. If the matter cannot be resolved to the client's satisfaction within 4 hours, the Office manager is involved to bring immediate satisfaction to the client. The issue and resolution are documented with a copy to the following:

- Client
- Investigator's File • Manager

ISSUE LEVEL 2, INTERMEDIATE ISSUES RELATING TO:

- Time Service (greater then 2 days)
- Personality Conflicts
- Not following Instructions
- Inaccurate Information

Resolution Processes: Level 2 issues are immediately brought to the attention of the Office Manager. They are resolved quickly between the manager and the client directly. If the matter cannot be resolved to the client's satisfaction within 4 hours during the French business hours, the Screening Operations Manager is involved to bring immediate satisfaction to the client. The issue and resolution are documented with a copy to the following:

- Client
- Investigator's File
- Office Manager
- Screening operations Manager

ISSUE LEVEL 3, MAJOR ISSUES RELATING TO:

- Security breach
- Privacy breach

Resolution Processes: In the case of reported Level 3 issues, such are immediately brought to the attention of ICOVER General Manager. Steps will be immediately taken to stop the breach and to ensure that no further breach can occur. They have immediate authority to direct all and any resources to ensure that client's data is protected. Contact is made with the Client's main representative to inform them of the situation and to advice on the following:

- What steps ICOVER has completed to minimize the exposure of data.
- What steps ICOVER will do to minimize damage from the breach.
- What steps ICOVER will do to ensure that this does not occur again.

5. INFORMATION SECURITY AND PRIVACY WITHIN OUR COMPANY

5.1. BACKGROUND CHECKS OF ICOVER EMPLOYEES

To provide consistent security levels throughout the company and in its offices, Background Checks are conducted on all company employees, agents, subcontractors and vendors who have access to customer and candidate sensitive data. The background checks include the following components:

- Education
- Employment
- Criminal

5.2. CONTINUOUS TRAININGS FOR SECURITY AWARENESS AND MAINTAINING PRIVACY STANDARDS

ICOVER organises training sessions on a regular basis for all company employees, agents, subcontractors and vendors and monitors compliance to the established security levels.

- Information security safeguards policy training: this is a mandatory training component before any employee access customer sensitive data.
- Trainings on privacy policies, procedures, and practices are organised regularly and whenever legal changes and technological updates appear

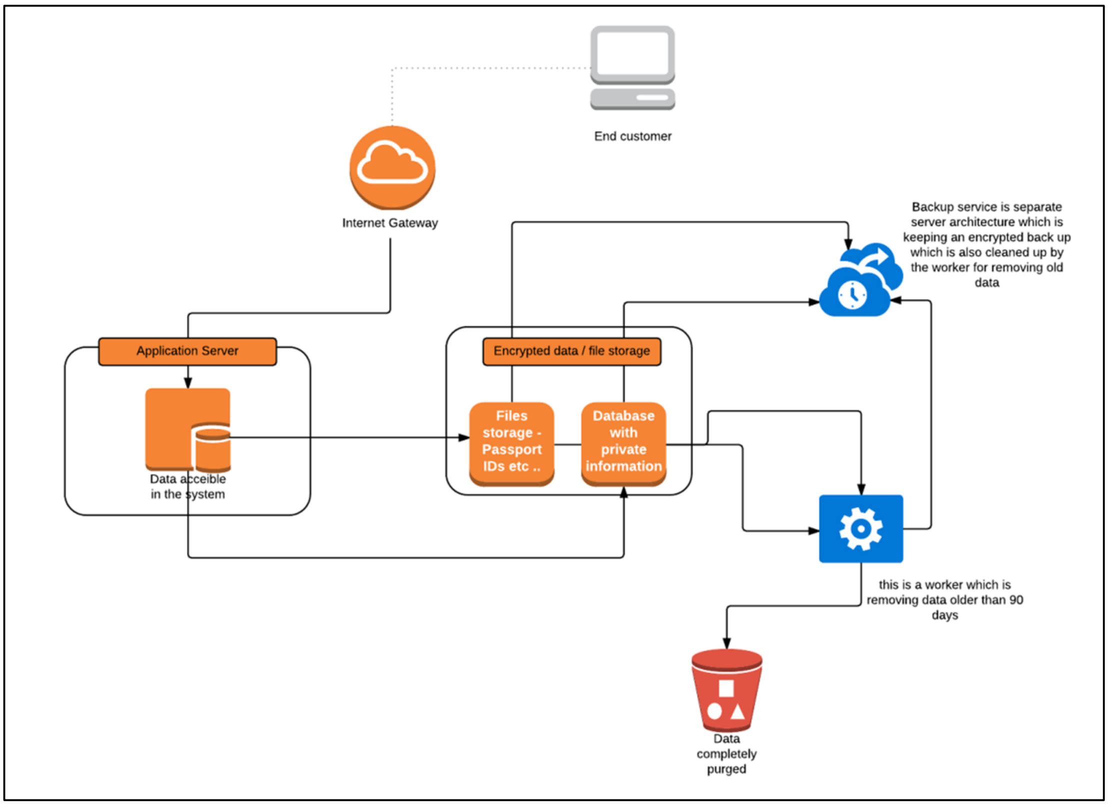
5.3 OUR DATA PRIVACY AND SECURITY PRINCIPLES AND THE INCORPORATED PRACTICES

- Collection, use, and dissemination of PII
- Compliance with privacy laws and/or regulations
- Regular review of privacy program and principles
- Individual data privacy Opt-Out Practices (Data Privacy Principles)
- Third-Party Service Providers information security and privacy safeguards
- Policy for restricting access to personal information to only those employees, subcontractors, and/or agents who need it as part of their job responsibilities
- Securing the protocols of data transfers to a third party providers
- Archiving
- Purging policy

5.4. PURGING POLICY

- ICOVER uses advanced system measures to protect Personal Data from loss, misuse & unauthorized access, disclosure, alteration and destruction
- Personal Data older than 90 days (3 months) from the production database is purged automatically on a daily basis
- Data purge is executed also for Server files uploaded 90 days ago, ensuring that there are no sensitive data records left with the ordered transactions
- The system runs the same process for all previous backups done for the storage system and database data
- In addition, the system runs clean-up scripts that are wiping specific data from previous backups, including the files that are archived into separate secured storage in a protected data centre.

5.5. GUARANTEEING INFORMATION SECURITY AND PHYSICAL SECURITY WITHIN OUR OFFICES (SAFEGUARD SHEET)


End customer
Internet Gateway
Backup service is separate server architecture which is keeping an encrypted back up which is also cleaned up by the worker for removing old data
Application Server
Encrypted data / file storage
Files storage - Passport IDs etc ..
Database with private information
Data acceible in the system
this is a worker which is removing data older than 90 days
Data completely purged

- Information Security and Physical Security Programs, including policies and procedures designed to help protect property and assets from unauthorized acquisition, loss, or damage
- Management of PII for Customers in a computer accessible format
- Policy on allowing associates to store PII on laptop computers and to remove such laptops from the premises
- Policies and procedures in place regarding required safeguards to prevent unauthorized access to, loss of, or theft of such laptops
- Databases and other data repositories containing, including all company servers, are secured behind firewalls
- Intrusion detection software is used between the Internet and these servers; this intrusion detection software used is kept current every year.
- Virus detection software installed on computer systems(s) is also used.
- Our Company has written procedures that cover the use of security technology to protect PII

5.6. REGULAR REVIEWS OF ALL INFORMATION SECURITY PROGRAMS & THE PHYSICAL SECURITY PROGRAMS

Our company is regularly scanned and certified by Acunetix. Our company has policies and procedures for handling information security breaches that may result in the unauthorized acquisition of consumer Sensitive Personally Identifiable Information (SPII)

- Our company has policies and procedures for notifying Customers and affected consumers in the event that Customers PII is lost, stolen or otherwise compromised in an information security breach
- Our company has policies and procedures to ensure employees, subcontractors and/or agents have access only to those Customers facilities or assets necessary to provide the service(s) your company provides to Customers
- Our company requires user IDs and passwords to control physical and information system access to Customers PII.
- Our company has minimum requirements for passwords, such as minimum length, alphanumeric combination, etc.
- Our company require passwords to be changed regularly
- Our company has policies and procedures by which physical and information system access privileges are rescinded upon termination, revocation of privileges, or reassignment of job responsibilities
- Our company has policies or procedures regarding the retention and/or disposal of physical and electronic copies of Customers PII
- These policies and procedures require shredding, degaussing, or other such means of destruction as appropriate.