2COMS Information Security Policy

Policy Owner – Bobby Das (Function Head – Technology)

Version 1.2

Published on: 19th April 2025

Last Reviewed: 14th August 2025

2COMS Consulting Private Limited (here onward mentioned as 2COMS) has implemented reasonable administrative, technical and physical safeguards (wherever applicable) to help protect against security incidents and privacy breaches involving any technical process generated for but not limited to manage Recruitment, Staffing, Skill development, Payroll, Compliance management, Attendance management, Manpower services, apprenticeship services etc.

However, as systems and threats evolve, no system can be protected against all vulnerabilities and we consider our clients, employees and candidates' data as the most critical aspect in maintaining security and privacy safeguards.

2COMS continuously strives to improve security and privacy throughout the service delivery and its continuous evolution using practices such as:

- Privacy and Security by Design
- Risk Assessment of involved parties
- Vulnerability and Patch Management
- Secure Coding Practices and Analysis
- Vulnerability Scanning and regular Audits
- Access Controls appropriate to Data sensitivity
- Incident Response
- Clear paths for two-way communication between stake holders and 2COMS If a privacy or security issue (incident, breach or vulnerability) arises.

The purpose of this document is to detail how 2COMS Information security have been applied for continuous protection against any threat which might lead to a compromised or impacted service delivery.

Service Delivery Application – Platform and Infrastructure:

2COMS has developed proprietary applications to deliver Manpower and Human Resource based services which are managed and hosted in globally accredited environment.

Servers housing the applications are hosted in Cloud Hosting Solutions always ensuring that the data resides in India. For AWS Cloud Services the Mumbai Datacenter is selected and for Zoho based SaaS services, their Chennai DC is currently hosting the data. By this process 2COMS adheres to our internal directive guideline of retaining data in domestic environment only.

Cloud hosted Servers are classified at medium to large levels depending on the type of service being delivered. Other resources are calculated on the server sizing based on the aggregated load expectancy for the said service by the business forecast models. For Zoho SaaS environments, the

vendor undertakes all the security and related purview. The documentation can be found here. Below documentation will continue to elaborate on the hosted environment scope.

Data Management:

Storage is maintained at two levels. For internal storage, AWS EBS volumes are used which are block level flexible devices. AWS Image based System Data is segregated logically or physically based on server implementation needs. Operating System information and structure is retained completely isolated from application data to ensure a contained environment in case of any infection related incident.

Application Data is stored in logically separated containers in each server based on stakeholder patterns. To ensure complete isolation, each application subset is defined to access specific data paths only which correspond to the required patterns. This data is maintained on a secondary storage level AWS S3. This data store also retains versioning to have redundancy.

Encryption:

Data is encrypted at rest and in transit. The algorithm requirements demand an adherence of ciphers in use to meet or exceed “AES-compatible”. The use of Advanced Encryption Standards (AES) is strongly recommended for symmetric encryption.

We use SHA-256 encryption method so that 2COMS Server admins can isolate control over access to the data, from access to the keys. This isolation model is a powerful additional logical separation control that is applied across 2COMS AWS server environment.

All Server remote connections are authenticated by encrypted certificates and are accessed by approved AWS Identities extended to each verified admins.

Network and Firewall:

The server structure is connected to internal and public network by AWS Virtual private cloud (VPC). The VPC allows the EC2 server structures to connect in a virtual network. The instance is configured with a primary network interface, which is a logical virtual network card. The instance receives a primary private IP address from the IPv4 address of the subnet, and it is assigned to the primary network interface.

Servers connect internally via private IP pool. For Public access, AWS Elastic IPs are mapped to the server instances.

Any external inbound or outbound connectivity is controlled by AWS security groups. A security group acts as a virtual firewall for the server instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to the instance, and outbound rules control the outgoing traffic. The rules can be applied on individual, lists of range of network ports limiting the access to fine grained level.

By default, public access is only allowed on the HTTPS or SFTP protocols for web login access. Rest of the ports are hardened and restricted from unauthorized access or bruteforce attempts.

Application Structure:

Database and Application Security:

By design, 2COMS applications have a database backbone maintained in SQL, MySQL or Maria-DB. Similar other database structures are also used as required by server scope. The log mechanism of MongoDB is also incorporated.

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. access by software programs must be granted only after authentication with credentials.

The credentials used for this authentication do not reside in the main, executing body of the program's source code in clear text or easily reversible encryption.

Database credentials are not stored in a location that can be accessed through a web server. Algorithms in use must meet the encryption guidelines. Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.

The credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.

The credentials do not reside in the documents tree of a web server.

Passwords or pass phrases used to access a database must adhere to the Password Policy.

The web server handling the UI and external public access of the application is mostly handled by apache, tom-cat or IIS and web management is done by CMS tools.

Security is managed via SSL certificates issued to each application enhancing the protection against malicious attempts.

Application Management and access controls:

The application is developed on tools with high reputation and industry standard practices. Entire coding is done by authorized developers who are verified and granted access post proper verification. Coding management, repository version management and collaboration is done via GitLab. provides end-to-end DevOps capabilities and for each stage of the software development lifecycle. It enables the development team to automate building and testing their code. Security capabilities are included with scan results presented to the developer within their native CI pipeline/workflow, and a dashboard assists with vulnerability management for the security testing.

Once any new code is developed for an upgrade or patch, it is reviewed by the security and implementation team. Post that it is uploaded to the development server and tested with rest of the environment. Post the same is validated and certified as stable by the review team, it is then scheduled for deployment and subsequently added to the production server by the upgrade team.

This two tier mechanism restricts access to the live environment from the development team from making unstable or unauthorized changes.

User / Access Management:

Access to the application is at multiple levels:

Privileged Access (All are internal Users):

Superadmin – Top level access with no restrictions to application and server structure.

Admin – Complete Application access but limited access to schema and structure.

Sr. Developer: Implementation – Access to both development and production server and all related codes in the repository.

Developer – Access to Code repository for their own codes or any code they have reviewed.

Apart from the above, non privileged users are created as part of the application who access the data records and handle day to day transactions.

All access controls are fine grained and defined as per CRUD logic at role as well as individual level. Entire access is defined on the principle of least privilege (PoLP). PoLP is an information security concept which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task.

Non Privileged Users are further differentiated on 3 grounds:

Internal Users: Users are internal employees of 2COMS.

Any Internal User (Privileged / Unprivileged) upon Exit formalities initiated, get moved to restricted permission mode and do not have access to sensitive data sets. Also day to day activities are defined keeping in mind the transient status of the user.

As all permissions are vested in the organization ID of the user, upon exit, all the access cease. The ID deactivation is a central procedure controlled the core Corporate HR and the Domain Admin team. Retention of IDs, transitional information and knowledge transfer records are taken up during the role handover by the Process Head and each and every pertinent information is securely transferred. Post that, depending on legal or organizational compliance rules, access IDs are retained or purged in due course.

End Users: This category refers to the user pool who interact based on credential generated on process action like staffing employees, apprentices, students, service partners who login to their relevant application for submitting their own documents / information securely into the system.

Access Control on this profile is very restricted and primarily does not allow any additional access beyond their own uploaded information. User deactivation is automatic on the process completion / expiry of the end user with 2COMS.

Customer Access: This user profile is mapped to external stake holders from customer organizations who either need to upload their information / process data to supplement existing end user data or to access reports or analytics if applicable. User deactivation is on express communication from the customer point of contact and/or completion or expiry of active agreement. Review team may

deactivate such access Users incase there is no login from these IDs for a continuous period of 3 months if the customer is active but not using the login. Reactivation can be easily done if required by a confirmation from customer end.

Business Continuity:

All the application modules and segments have failovers and backups defined on volume level and instance level. A complete lifecycle is setup to maintain a backup sequence keeping a series of recovery points over a set period.

Backups are also periodically checked by the internal team for regular test recovery, bare metal recovery, file level recovery and code repositories.

Server Security and vulnerabilities:

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

All application servers deployed are owned by an operational group that is responsible for system administration. Approved server configuration guides are established and maintained by each operational group, based on business needs, and approved by the Implementation team. Operational groups monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group establish a process for changing the configuration guides, which includes review and approval by the Domain Head.

For security, compliance, and maintenance purposes, authorized personnel monitor and audit equipment, systems, processes, and network traffic during the quarterly review meetings.

Server System configuration are done accordance with approved internal guidelines

Services and applications that will not be used must be disabled where practical.

Access to services are logged and/or protected through access-control methods including web application firewall.

The most recent security patches are always installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

Standard security principles of least required access is used to perform a function.

Restricted use of root when a non-privileged account will do.

If a methodology for secure channel connection is available (i.e., technically feasible), privileged access is always performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

Application Data Handling:

No unauthorized personnel are allowed any access to the application data. The same is achieved by stringent security measures at the server side by general hardening, usage of identities, access certificates and authentication passphrases. At user side, all credentials are backed by multi factor authentication method. Each employee is hard coded to a mobile number and email ID tagged to

them. The mobile number and email ID is provided by HR after validation to ensure no gap or incorrect mapping happens.

Records handled by the system users have versioning history to ensure unbroken change log and a fine grained audit trail with user identity attached. Any change to any data record will be traceable back to the user along with the timestamp of the change and the fields impacted.

Data records are handled entirely in the web application accessed by the candidates and the authorised users. The system absolutely restricts the ability to download and retain any data record in native or excel / csv format. Any changes / modifications to the record are subject to the role assigned to the user and entirely happen within the web interface. All authorized users are also governed by employee monitoring tools and endpoint control applications for internal performance management. This further controls and restricts the user from using any unauthorized data capture methods

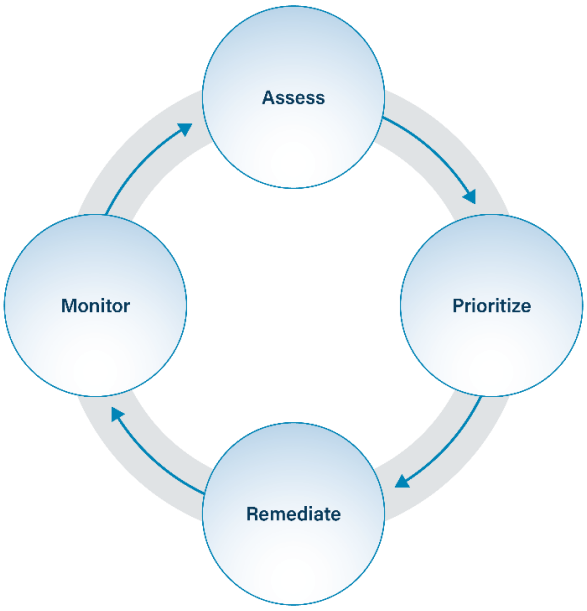
All data access, system, security and application logs are maintained by syslog services and are retained for a minimum of 90 days or 120 days depending on the criticality of the servers.

All logs are periodically audited by the internal review team not less than once in a quarter. Any variations from the median or expected patterns are highlighted and discussed during the subsequent meetings with the development team. Any anomalies or deviances which need further check are investigated and if required, then submitted to Domain head and the Management for advice. Based on the top level guidance provided, corrective actions are taken.

All security-related events on critical or sensitive systems are logged and audit trails maintained. Security-related events are reported to the review team, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to: Port-scan attacks, evidence of unauthorized access to privileged accounts, Anomalous occurrences that are not related to specific applications on the host.

Vulnerability Assessment and Management:

2COMS vulnerability management guidelines cover multiple sections based on usage patterns of Servers and other IT assets. Below is a pictorial depiction followed by a detailed description of what each step entails.



- **Assess** – A combination of automated scanning, manual analysis, and leveraging threat intelligence to ascertain if vulnerabilities exist in the servers and housed software.
- **Prioritize** – Creating a prioritized list of vulnerabilities that should be remediated in a specific order. This may simply be identifying and fixing critical vulnerabilities first.
- **Remediate** – Fixing or patching vulnerabilities to ensure they are removed or mitigated in some other way.
- **Monitor** – Ensuring that remediated vulnerabilities are no longer affecting systems or did not introduce more problems that must be solved.

Assess

2COMS Admins assess their infrastructure for vulnerabilities and proactively address discovered flaws via industry standard vulnerability scanning tools. They also rely on global threat intelligence sources provided email lists, blogs, open-source intelligence (OSINT), or other data sources to base their findings to validate and compare with vulnerabilities in software and the servers. To help standardize the definitions of discovered vulnerabilities across the organization, Admins map vulnerabilities to industry-recognized vulnerability rating, configuration, and classification schemes/languages.

Prioritize

Once vulnerabilities are identified, they are fixed, code based patches deployed, or remediated. Once vulnerabilities are identified, internally they get mapped as incidents, prioritized, and correction procedures are mapped. Once a stake holder is appointed to the incident, depending on the criticality, a schedule is set. This helps to close minor gaps on standard patch management cycles and to highlight unmitigated critical vulnerabilities to senior management to ensure they are resolved. The turn around time for rectification is mapped for future incident comparisons and are used for documenting internal compliance requirements to showcase remediation efforts based on business impact.

Remediate

Security patches are implemented as updates to the server / system's operating system (OS) or installed software applications and are a basic part of Information Technology (IT) maintenance. The patches that developers provide often contain new features, but also contain fixes to recently discovered security vulnerabilities. Patching can be performed with patching tools, added code modifications or be configured in the operating system of a device.

Some operating systems and application platforms provide auto notifications on available upgrades, patches or version updates. These help in scheduling regular management. Proprietary application code changes and patches are reviewed in earlier discussed process and then pushed for production deployment as per planned maintenance windows.

Monitor

2COMS deploys the internal review team for quality assurance process which verifies that patches and updates are implemented correctly and across all relevant Servers and applications including planned updates and upgrades. Monitoring ensures that patches correctly fixed identified issues and server/service/application in question no longer requires further service. This includes the continuous process of re-evaluating assets that have already completed the vulnerability management process, which then leads back to the asset assessment process. As this occurs, data is analysed that can further identify vulnerabilities through Security Information and Event Logs.

The entire cycle is a regular internal activity and is set to run on a continuous basis. Monitoring is assisted by system notifications on the availability of critical updates as well. Maintenance windows are scheduled once in every two months and all updates applicable till then which do not impact undisturbed business process are deployed during the same. In case of urgent deployment needs, immediate schedules are planned and run during non-business hours. Unless impacting any stake holders directly in their day to day business functions, most of the patching activities are run internally. In the event that the version upgrade has applicable features or timelines impacting the external pool, notifications are sent out with keeping a minimum of 7 business days.

Secure Development:

Software assurance encompasses the development and implementation of methods and processes for ensuring that software functions as intended and is free of design defects and implementation flaws.

2COMS ensures secure software development and includes updates to the fundamental practices to reflect current best practice, new technical considerations and broader practices now considered foundational to a successful Secure Development Lifecycle (SDL) program.

• Requirement Identification

• Management of Third-party Component Components (both Open Source and Commercial Off the-shelf)

• Security Issue Management

• Vulnerability Response and Disclosure

Each change / development requirement identified is tracked through implementation and verification in Gitlab which acts as our coding repository as well as an Application Development Lifecycle Management (ADLM).

Keeping secure design principles as guidelines, 2COMS coding and development team follows the below elaborated procedures:

• Economy of mechanism: keeping the design of the system as simple and small as possible.

• Fail-safe defaults: base access decisions on permission (a user is explicitly allowed access to a resource) rather than exclusion (a user is explicitly denied access to a resource).

• Complete mediation: every access to every object must be checked for authorization.

• Least privilege: every program and every user of the system should operate using the least set of privileges necessary to complete the job.

• Least common mechanism: minimize the amount of mechanism common to more than one user and depended on by all users.

• Psychological acceptability: The UI and UX is designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

• Compromise recording: The concept that reliably record that a compromise of information has occurred can be used in place of more elaborate mechanisms that completely prevent loss is adapted as per applicable situation.

• Apply encryption strategy defining what to protect, designation of mechanisms to use for encryption, having a key and certificate management solution and Implement with cryptographic agility in mind.

• Establish Coding Standards and Conventions

• Use Current Compiler and Toolchain Versions and Secure Compiler Options

• Use Code Analysis Tools to Find Security Issues Early

• Standardize Identity and Access Management

Open Communication:

Communication on incidents and Information security status changes are made based on the below matrix:

Issue Category	Implementation Team	Review Team	Development Team	IT Team	Management	Business Head	Process Head	Project Manager	Technical Head	Client	Candidates / User Pool	Cloud Support
	2COMS Technical Team				2COMS Internal Stakeholders					External Stakeholders		
Incident												
Individual User Impact		I	A	R								C
Partial Service Impact	A	C	A	R		I	I	I	A	I	I	C
Global Level Impact	A	C	A	R	I	I	I	I	A	I	I	C
Updates and Maintenance												
Planned Maintenance / Daily updates		I	A	R							I	
Server Schema changes / Maintenance	A	C	R	R				I	I		I	
Security Patches / Vulnerability fixes	I	C	A	R							I	C
Critical Urgent Updates (service downtime)	A	C	R	R	I	I	I	I	C	I	I	C
Upgrades												
Scheduled upgrades with patches / bugfixes	C	A	R						I			C
Major Development Deployment / Critical Service Correction	R	A	R		I	I	I	I	C	I	I	C
Data Breach / Security Issue												
System generated issue leading to data changes / Data structure not impacted	C		A	R			I	I	I			C
Data Impact / Security Issue RCA and Scrutiny required with deep investigation	A	C	A	R	C	C	C	I	A	I	I	C

Concluding Remarks

2COMS prides itself on maintaining proper security of its services. Addressing any and all privacy concerns of our service stakeholders is among our top priorities. 2COMS has carefully studied the current applicable data security laws and guidelines.

We appreciate you taking these issues as seriously as we do. If any questions or considerations have gone unanswered in this document, kindly drop a mail to it@2coms.com. We will gladly consider and review them and include in the next iteration.