Comintelli Policy on IT and Security

OFFICE AND PERSONNEL

1. Office physical security

Intrusion protection

The office is protected against unauthorized access by a multi-tier solution for perimeter protection. The entire building complex is guarded 24/7/365 by patrolling guards and entrance monitoring. CCTV monitoring of facilities both externally and internally is in operation and footage is archived for up to 10 days. Access to the main building entrances requires a key card after office hours. All People working in the facility have access to the main area. The D-building (in Which Comintelli resides) elevators are accessed through a locked door accessible with a valid key card. Only people with offices related to the D-building have access. The office floor's common areas are accessed through a locked door with a key card. Only three companies have access to this area. Anyone not recognized as normally having business in the area must be challenged by the staff who should, if deemed relevant, notify security personnel. Visitors register in the main building reception before entering any of the office areas and are accompanied by the host during the visit.

Comintelli's office area is accessible with the same key card, but only employees at Comintelli have access. The door shall be locked and must not be held open, even under shorter periods of time for example when leaving the office for the restrooms or for the meeting room area. Access to server rooms are permitted for authorized personnel only and audited regularly.

Issue, activation, de-activation and return of key cards are done according to audited documented procedures

Fire

Fire extinguishers shall always be available at the office entrance. One fire extinguisher is for fires in electrical equipment (carbon dioxide) and one for other fires (light water/"foam"). Both are regularly checked and exchanged according to instructions by the fire authorities.

Electrical installations

All electrical installations shall be performed by a certified professional and all electrical equipment shall be S or CB or CE certified.

Clean desk

Computers, laptops, tablets and phones must be locked with at least password when workspace is left unattended. Passwords may not be left written down in any visible/accessible location.

Employees are required to ensure that restricted/sensitive/confidential (hereinafter "Restricted") information in hardcopy or electronic form is removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

File cabinets containing Restricted information must be kept closed and locked when not in use or when not attended and keys used for access to such cabinets must not be left unattended at any time.

Printouts containing Restricted information should be immediately removed from the printer. Upon disposal such documents should be shredded in the office shredder. Whiteboards containing Restricted information should be erased immediately after usage, and always after meetings in conference rooms.

All mass storage devices such as external hard drives or USB drives are to be considered as Restricted information and handled as such.

2. Routines for change of employment status

Leaving the company

When an employee leaves the company, a revocation of systems access and hardware is performed on the last day of employment. All company owned hardware and tools shall be returned to the employees Manager.

This includes:

- Computer
- Mobile Phone
- External storage media (disk, USB drives, memory cards)
- Printed corporate documents
- Keys and access card
- Other tools applicable

Upon leaving the company, the employee signs a document warranting that all internal and Restricted information has been returned to the company and that no such information in any way has been, or will be, transferred from the company in conjunction with the employees foregoing employment with the company.

Change of position

When changing a job position in the company, systems access is re-evaluated by the employees Manager and any changes deemed necessary are implemented.

3. Personnel Security

Education, work-related and relevant security background checks are conducted on all employees (Temporary or Permanent) prior to any engagement with the company. All employees sign the terms of employment, which include provisions to protect Restricted information as well as to adhere to this and all other company policies and instructions. All employees must undertake security awareness and education training upon the start of employment. Such training is updated with all employees at least annually.

OFFICE IT

4. Office Hardware

All computers (clients and servers) must have company approved antivirus and firewall software installed, updated and activated. OS updates and security patches are to be installed immediately upon availability. A company computer may only connect to networks with encrypted communication and firewall protection. The use of free and open public hotspots is not allowed. The servers are protected by a separate advanced firewall solution provided by the server hosting company. Unique user IDs and strong password controls are implemented and remote access is strictly controlled.

Employees are not allowed to share access credentials with any party, run password checkers on system password files, run network sniffers, break into other accounts, disrupt service, abuse system resources, misuse e-mail (spamming or illegal activities), examine other user's files unless asked to do so by the file owner or manager, copy unlicensed software or allow other users to copy unlicensed software. Passwords shall meet the Comintelli

minimum requirements and may not be reused on multiple instances. Two factor authentication is enforced to access corporate accounts and assets.

5. Office Software

Employees may install different software packages on their office computers and mobile devices depending on professional needs and preferences. Only legally procured and safely downloaded applications can be installed. All such software shall, prior to installation, be cleared by IT as secure and approved.

Information Management and classification

All major information assets shall have an owner. The owner shall classify the information depending on legal obligations, costs, corporate policy and business needs. He/she is responsible for the protection of this information. The owner shall declare who is allowed access to the data.

Public Information

Systems containing public information could be publicly available without any implications for the company. In such systems, data integrity is not vital. Loss of service due to malicious attacks is an acceptable, albeit managed, risk. Examples: Test services without confidential data, certain public information services.

Internal Information

Unauthorized access to this data is to be prevented, but should this data become public, the consequences are not critical. Internal access is selective. Data integrity is important but not vital. Examples of this type of data are found in development groups (where no live data is present), certain production public services, certain "normal" working documents and project/meeting protocols and internal telephone books.

Internal information should regularly be scanned for viruses. Information shall be labeled. i.e. the classification level should be written on documents, external storage media, electronic messages and files. For projects involving collaboration with external partners, a project policy document shall stipulate what information may be shared with the external partners. If such information must be transmitted through public media (e.g. the Internet) it should be encrypted. Internal data shall not be transferred outside the company except mentioned above.

Restricted Information

Restricted information should be strongly protected from unauthorized access. If such data were to be accessed by unauthorized persons, it could influence the company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause considerable damage to customers or other third party business associates. Data integrity is vital. Examples: Salaries, Personnel data, Accounting data, sensitive projects and confidential contracts. All Customer Data and customer commercial information are by default deemed Restricted information.

Restricted Information shall be labeled, i.e. the classification level should be written on documents, external storage media electronic messages and files. Storage susceptible to virus attacks should be regularly scanned for viruses. The integrity of systems should be regularly monitored. IT Systems shall be configured to protect against unauthorized modification of data and programs. Physical copies of such information shall be kept under lock and key (e.g. documents in fire proof safes, computers in locked rooms). If such information must transit public media (e.g. the Internet), it should be encrypted.

Restricted information shall be securely disposed of when no longer needed (e.g. shredders for documents, physical destruction of old disks and diskettes etc.).

6. Encryption

Offline information, synchronized from the Cloud Server is stored in encrypted form on local hard drives or any other local device. Other Comintelli related information stored on the local devices is encrypted using the BitLocker encryption system in Windows. Backup copies are not encrypted, but stored safely, without direct access. Communication between the Client and Cloud Server must always be encrypted.

7. Backup – Office Data

The backups of the cloud stored content are stored for 6 months. All office computers are backed-up online via Google Drive, in order to prevent data loss due to virus attacks, computer malfunction or loss of computer by theft or accident, long time absence or death of an employee. Files and Data must be stored at least on two different locations simultaneously to be considered to be backed up. Due to the risk of theft and fire or data corruption, backups shall not be stored together with the computers.

CLOUD IT

This Cloud IT section of this policy covers the provisioning of Cloud Services for Intelligence2day®

8. Systems Management

Server operating systems are to be patched on a monthly basis. The application platform is patched when high security patches are available. Patches related to the application server, database engines and search engine, are implemented after staging of the update and when the patches are relevant. All updates and patches are logged.

Corrections related to errors in the Intelligence2day® source code are applied with different priority.

Non-disruptive bugs and non-security related bugs are patched, along with potentially new code such as feature enhancements and additions, during scheduled service windows as planned with customers. Disruptive bugs and security patches are handled as priority support tickets for each customer.

9. Systems Access

The SaaS platform is maintained exclusively through a VPN connection using SSH to a Bastion host that provides a single point of fortification.

Only authorized personnel are allowed to access the servers. Personal user accounts should be used to trace actions. Customer Data may only be accessed by Comintelli personnel on request by a customer and only in order to help solve problems related to the system. Comintelli applies the principle of least privileges, which translates to giving a user account only those privileges which are essential to that user's work.

The only permitted method for remote server access is encrypted connectivity. Authentication policy for remote access employs strong complexity requirements. Minimum authorized access is provided with clear segregation of duties and formal request processes for the extension of access and/or changes to access requirements are established.

Customer access to the Cloud Service is always encrypted through a 256 bit SSL connection.

If other SSL certificates should be applied, this needs to be done on a dedicated server and that the Customer must supply a valid certificate.

10. Firewall Protection

All servers and services are protected by firewalls and similar technologies. By default only the minimum number of ports are exposed to the internet. Ports to be opened are defined in a confidential firewall policy document. In addition a local firewall is installed on each server on Windows based servers.

Depending on the purpose of the server, IP restrictions may apply for accessing the server. A dedicated customer server should be restricted by the IP domains for this customer and Comintelli support staff.

11. Server Intrusion detection

Intrusion detection systems (IDS) are active on all Windows based servers. IDS log files are analyzed on a regular basis. Excessive login attempts should be blocked on an IP level and manually or automatically added to the firewalls block list.

12. Backup – Cloud data

Data on Intelligence2day systems is backed up daily and stored for 30 days on physically separated instances.

Systems Performance and Availability

The systems shall be available 24/7/365. Monthly service windows should be planned and communicated to Clients. Standard monthly service windows are approximately 30 minutes per month.

Customer Data

All Customer Data stored in the Cloud Service (automatically and manually published articles and documents) is the property of the customer. The customer is fully responsible for any copyright or other infringements that may apply. Each customer's Customer Data shall be separated from other customers' data. Customer Data shall only be used for its intended purposes, unless specifically specified by a customer

Certificate Compliance

Comintelli maintains a range of strict internal policies covering aspects from IT- Security and Disaster Recovery to personnel and office routine requirements. Subcontracted providers of IT cloud environments are required to either adhere to, or to be certified according to, relevant standards such as ISO 27001 and/or SSAE16 (SOC2).

Customers of Comintelli's Cloud Service solutions may at any time be required to be presented with proof of any such policies or certificates. Further, although current standard hosting is ISO 27001 accredited, customers are welcome to discuss other options depending on preference.

Comintelli itself is not formally accredited with ISO certificates or SOC assessments but it is the company's outspoken intent to, to the extent possible, adhere to such policies as relevant and to maintain a level of compliance that would be sufficient for a formal ISO or SOC accreditation.

Secure Software Development

Comintelli acknowledges the importance for security at every phase of the software development. In this context, we pledge to take all precautions related to security in all work processes of the software development life cycle and to Follow our IT & Information Security policies at https://comintelli.com/termsandpolicies/

Comintelli has training sessions annually in order to ensure that all employees and business partners understand the security risks and how to mitigate them.

All backend end points such as databases, search indexes, diskstorage and server management interfaces, are restricted to authorized personnel via VPN and personal authentication.

Technical details and data related to the application, are restricted to authorized personnel.

Developers must ensure that all the steps of secure software development are carefully carried out during development of code.

The Management Team pledges to communicate this policy to all employees, and to make sure that this policy is understood by all employees. This policy constitutes a framework for the targets and is reviewed continuously.

13. Application Development

Minor features may be decided by the Head of Development and major features are decided by the Product Team

14. Application Security

All access to data that is not classified as public, must be secured by authentication, with correct rights and roles and only be provided by the security framework in the application.

15. Logging of events

All logon events, successful and unsuccessful attempts are logged.
All usage of elevated privileges such as deletions and modifications of data are logged with time, userid, type of operation and affected objects.

16. Data encryption

Data in transit shall always be encrypted and the HTTPS protocol is used where applicable and available.
Where encryption at rest is not available data classified as sensitive, should be stored in a best practice encrypted format.

Sensitive data stored in the database or local storage, such as passwords and API keys shall be encrypted. User Passwords must be stored with best practice irreversible hash strings. Insecure methods such as MD5 hash are not allowed.

All response objects produced by the applications shall undergo output coding controls and in compliance with General Data Protection Regulation (GDPR), unauthorized persons are prevented from viewing personal data.

17. Coding security

All committed code is reviewed by another developer and tested in two steps, developer test in development environment and in the staging environment by both Comintelli personnel and external resources.

User inputs which the users carry out via interface or which can be accessed by parameters due to system structure in the applications, is validated and tested both for SQLInject or other manipulations and user errors.

18. Third Party Software

Each Server Software or javascript plugin used must be validated, secured and documented. Active plugins must be promptly updated when there are security fixes available. Third party Licensing is always validated and documented.

The general policy is that third party plugins shall be avoided when possible.

19. Third Party Services & Content

Imported content must be sanitized and secured from javascript, iframe and other potential threats.

Implementation of third party services must be cleared by the Product Team and carefully validated and before implementation.

20. Source code management

Source code changes within the development lifecycle are logged and managed through formal change control procedures. Each new code set renders an updated SVN identity. Each instance implemented in a production environment can, at all times, be traced by its unique SVN identity.

21. Vulnerability testing

To be OWASP compliant, automated software tools are used for vulnerability and penetration tests.
Each new standard edition of Intelligence2day® is tested for vulnerabilities, both on application level and infrastructure. Test procedures include a wide variety of possible vulnerabilities including but not limited to Command and SQL injection, cross-site scripting, security misconfiguration, sensitive data exposure, cross site request forgery, parameter tampering, unvalidated redirects and system vulnerabilities.

After final completion of an Intelligence2day® edition, the results are released in a Vulnerability Report to all Customers and in some cases, prospects where NDA agreements are in place. Security findings with high impact are remediated in a timely manner.

22. Responsible Disclosure

Comintelli does its utmost to keep its software and services safe for all and it is recognized that security is of the highest priority. In spite of the care and efforts taken for the security of our systems, it can happen that a weak point remains. In addition to Comintelli's vulnerability testing Customers are encouraged to actively search for vulnerabilities in our products and services and we appreciate any disclosing of findings in a responsible manner, so that adequate measures can be taken to resolve such matters. Comintelli takes security issues seriously and will respond swiftly to fix verifiable security issues. When properly notified of legitimate issues, we will acknowledge any emailed reports, assign resources to investigate the issue and fix potential problems as quickly as possible. Our responsible disclosure process is hosted by Zendesk and customers may file vulnerability findings to support@comintelli.com.