



# Comtek International Inc.



## Security and Disaster Recovery

### Infrastructure & Security

As a provider of offshore software development services, we have developed an understanding for our client's fears and worries. We know that delegating any part of your own software development is an intimate process. Here, we have gathered some facts to demonstrate how we cherish the security concerns of our clients, eliminating the risk of losing data and suffering from unprotected intellectual property rights.

### SDC Security

Comtek's St. Petersburg development center is located in a secure modern office building. The building was fully renovated in 1998. The building's other tenants are primarily Western companies. Building access is controlled by security staff 24x7 and is based on strict photo identification. protected by advanced access control systems, offer comfort to our employees and support high productivity. The level of infrastructure availability at Comtek is 99.8% throughout the year.

Comtek International office premises in St. Petersburg, Russia are we maintain all necessary continuity plans and actions to ensure continuous operations. VPN provides secure global connectivity to remote users, tele- and videoconferencing. Comtek premises are protected from intrusion, and welcome client inspections and audits.

Comtek is a US based company as well as the St. Petersburg development center. Comtek will provide contractual assurance of data security as well as backed by insurance.

### Communications

Comtek uses digital phone lines for voice communication. In terms of Internet connectivity, Comtek's offices have 2 independent high-speed ADSL links to different providers.

### Network security

Comtek uses secure network architecture to ensure protection of all its systems, networks, applications, and intellectual properties. This security architecture is emulated in various configurations throughout Comtek. The core architecture uses the following components:

1. Connection Points - External routers provide a connection between Comtek's network and the Internet and provide basic protection (based on packet filters) from traffic spoofing.
2. Our firewall is the first line of defense for our network to prevent unauthorized access (penetration) from external entities and controls internal traffic policy. Our firewall policy is based on communications protocol, traffic source and destination, and protocol state restrictions.
3. The Network Address Translation function and our Proxy ensure a higher level of network security during communications between the Comtek LAN and external resources.
4. Tunneling. We use tunnels for connecting our premises with common computing networks through the public Internet. Our tunnels are built on the Ipsec protocol and provide 128-Kb traffic encryption. In addition, we maintain a secure VPN between Comtek's Chicago and St. Petersburg offices.
5. PartSecure Segments. The PartSecure Segment is a portion of our network that is in essence a protected firewall system. The computing systems on this network have direct access to/from the Internet and are

6. typically used only for demonstrating our products to customers.
7. Authentication Authorization Accounting (AAA) Domain. A user (Comtek employee, customer, partner etc) gains access to computing resources after authentication (based on login/password and source control schemas). User is also verified to have permission to use the resource through an access list. All important user actions are logged. Comtek's AAA domain is implemented using Microsoft Active Directory on Microsoft-based computers and other variants (local authorization, RADIUS-server) on non-Microsoft platforms.

## Data Security

A backup solution for all Comtek premises is a backup server employing a tape device (DDS-3, DDS-4 or DLT). Backup and recovery procedures have been established and tested for each type of data. The following is covered with backup:

- Data storage (database, file, mail, source-code servers)
- Servers and workstations (operating system data and workspace)

All backup tapes are stored outside the company's facilities in a secure location. Backup procedures run automatically, with periodic manual control based on daily, weekly, monthly, and yearly backup sets. Also, at the end of a project, all project-related data (source code, documentation, databases etc.) are burned into CDs.

The type of backup data can be changed by request from the project team (at the beginning or the end of the project, change of the computer environment, etc.) and validated by system administration team on periodic basis (e.g. once per month).

Recovery from backup is performed by a system administration team in cases of hardware failure or by client request.

## Disaster Recovery Plan

The disaster recovery plan addresses the following areas:

1. Hardware or software failures, data losses during development work at the Chicago office. A dedicated System administrator is responsible for hardware, software, or data failures. System admin restores data from backups that are stored outside of the office. System admin is also responsible for synchronizing information between the offices.

Comtek maintains 3 server sets:

- a. Development and demo servers at St. Petersburg office
- b. Demo servers at Chicago office
- c. Demo servers at independent provider (partner company) in St. Petersburg (Comtek, Ltd).

When required, development or demo sites are quickly transferred to one of the backup servers. No development is performed on developer's workstations. All project information (including documentation and code) is on development servers that are covered by a continuous backup routine.

2. General office building problems (fire or other)

Every member of the development team has a computer at home equipped with dial-in Internet connectivity, which shall be used in case of any general office problems.

External server platforms (office in Chicago and Valsset, Ltd.) are used to restore the team development environment from the backup.

3. Internet connectivity problems

In St. Petersburg, there are two independent channels. Should one of them go down, dynamic routing transfers all traffic to the other ones. If both lines are down, the office has dial-up connectivity for critical tasks.

In Chicago, SBC/Ameritech support is used to resolve office connectivity issues. In the event the link is down during office hours, Chicago staff uses dial-up access.

4. Staff migration

Comtek maintains long-term contracts with employees. This ensures that we have minimal staff turnover. As a rule, a person finishes all his tasks and shares his knowledge with others before leaving the company.

In each project, a senior manager supervises the process. He is always up to date with project requirements and status. In the event a team member gets sick or unexpectedly leaves the

company, he initiates replacement and knowledge- sharing processes.

## Technology Risk Management

Comtek takes great pains to ensure that its process is running properly and that the final product is of the utmost quality.

Projects that provide and describe standard processes have checklists and assessment schedules as inseparable parts of the contract; assessments are held according to a coordinated schedule; reports are delivered.

In processes wherein a standard process is not explicitly provided for, senior management performs routine project checks (at least once every two weeks, for short or urgent projects periodicity can vary from once a week to once a day). The following process areas are checked:

- a. SCM (checks if version control systems are used, backup procedures, document storage, bug tracking)
- b. Requirements management (quality of specifications, whether client interaction is smooth, whether the customer is actively involved in evaluating intermediate versions and testing)
- c. Process & Resources (whether any important project phases have been forgotten; whether all necessary roles have been defined and assigned; whether all participants are properly

qualified; whether PM records are being filled out properly)

- d. Planning, Schedule & Deliverables (whether the plan is kept up-to-date; whether everything is being accomplished according to schedule; whether all deliverables are delivered as promised)
- e. Communications (whether there is a mailing list; whether all correspondence goes via the list; whether client interaction/communication rules have been established and communicated; whether client-side contacts are responding adequately; whether status and review meetings are being held)

## Intellectual Property Protection

For the last 15 years Russia has been an integral part of the technology and IP portfolio for such technology giants as Intel, Motorola, and Sun Microsystems, just to name a few. International IP transactions involving technology acquisitions routinely take place in Russia. Leading international law firms (e.g. Baker & McKenzie, Gowlings, Deloitte, etc.) have developed practical proof that the intellectual property (IP) laws currently on the books in Russia are compliant with International intellectual property laws.

## Russia: Top Networking Facts:

- Mobile phone penetration is higher than in major U.S. cities: 70% in Moscow compared to 54% in New York City
- VoIP is growing in Russia: The largest market in Europe, 6th largest in the world
- Broadband is widespread: Over 1,250,000 active xDSL lines
- Wi-Fi has local concentration areas: Moscow and Saint Petersburg
- Top IT schools are in top IT cities: Moscow, Saint Petersburg and Novosibirsk
- Telecom is covered by multiple regulatory agencies: Ministry of Telecommunications, the Security Council, Duma Committee on Information Security, etc.
- The year-over year growth rate of weekly Internet viewers is 85% in 2005, with the number of subscribers estimated at 18.5 million (a 13% penetration)

## Minds without Borders