



*Behind Every Business Decision*

## **System Description of The NPD Group Information Technology Environment**

The NPD Group is a global market research company that leading companies turn to and rely on for essential market information to help them make their most important business decisions. Clients use NPD information to uncover market opportunities, strengthen channel relationships, and benchmark industry performance.

The purpose of this system description document is to represent NPD's IT infrastructure in accordance with the practices of the SysTrust® audit certification. Described in this document are the environments and processes supporting our Data Centers for network, storage, and server. Also included are the practices of the corporate Helpdesk, change management, system monitoring and security.

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- People (developers, operators, users and managers)
- Procedures (automated and manual)
- Data (transactions, files, and databases)

The following sections of this description define each of these five components comprising the system.

### **Infrastructure**

NPD IT Infrastructure includes secure data centers, located in New York and New Jersey. Housed within the data centers are the supporting operating system platforms (Windows, UNIX and Linux), disk/tape storage devices and networking components (firewalls, Intrusion prevention systems, routers, switches). The data centers are linked by high speed private IP wide area networks and d-VPN tunnels to our field offices throughout the global NPD presence. NPD staff that support the data centers are primarily located in our corporate headquarters in New York. Other IT staff are located at various remote offices to allow for additional time zone support coverage.

NPD can be characterized as a data warehouse organization with systems receiving data from our client base, ETL processing systems to reorganize the data received, databases to categorize the data and delivery systems to present the data back to clients. Internet technologies such as SFTP and WWW (SSL) are used as input and output of the NPD information processing system.



*Behind Every Business Decision*

Server technologies processing NPD data are centralized in the data centers to ensure uptime, security and production on-time delivery. The servers are summarized below by operating systems and various purposes of the systems:

- UNIX
  - HP-UX
  - IBM AIX
  - FTP services
  - Backup/Restore services
  - Monitoring tools
  - Data analysis software applications
- Linux
  - Red Hat - RHEL
  - Data processing applications
  - Database servers
- Microsoft Windows
  - Standard and Enterprise
  - Monitoring tools
  - Middle tier application data delivery servers
  - Terminal server application portals

## **Software**

NPD's information processing applications are based on state of the art ETL processing, analysis, and delivery systems with development efforts provided in the NPD headquarters. Software is largely custom written to meet the functional and performance requirements of our clients. Market information is received by NPD, processed and returned to our clients via our information processing systems. The system accepts data from digital files transmitted via the telecommunications infrastructure, input into the data record matching process, exported to data quality processes, and then run through ETL systems. Data are then uploaded to database and data mart environments to produce reports by business, frequency, and data type. Analytics are run against the information for enhanced study on market trends, positions and other valuable intelligence for our clients.

Other IT software used by NPD to support its information technology infrastructure include:

- Job scheduling, processing, and monitoring
- System, network, and security monitoring
- Helpdesk and change management
- Storage Management



*Behind Every Business Decision*

## People

NPD personnel provide the following core support services over the data processing and IT infrastructure.

The Information Technology team has the following responsibilities:

- Information Security and Risk is responsible for security administration, security monitoring, documented policies and procedures. The Helpdesk provides technical assistance for all NPD users and clients
- Desktop Support provisions staff information technology devices and provides high level technical support to NPD staff
- Server and Storage Support manages and monitors all server systems and storage arrays
- Voice and Data Network staff maintain all communication equipment, monitoring and telecommunication lines
- Data Center team provide backup and recovery services, 24x7x365 data center operations
- Facility Management maintains all building access, physical building infrastructure and workplace conditions

The NPD Engineering team provides services such as:

- Database Administration team manages, monitors all database related activities
- Development and Application Design group provides all in-house software tools, enhancements, fixes, documentation and modifications to the processing factory
- Analytics Support helps NPD staff use advanced tools

The NPD Operations team provides services such as:

- Production Support manages job queues, system processing schedules, programming of custom and syndicated client deliverables
- LOB Deliverables Processing, in each LOB, supports client deliverables and quality of data for on-time delivery and correctness
- Data Quality monitors compliance with NPD standards testing all software changes, system related changes and automated job processing



*Behind Every Business Decision*

## **Procedures**

NPD has documented policies and procedures to support the operation and controls over its IT infrastructure environment managed by the IT team. Specific examples of the relevant policies and procedures include the following:

- Information Security Policy
- Moves, Adds, Changes Policy
- Software Code of Ethics
- NPD Software Policy
- NPD Technology Policy
- Acceptable Use Policy
- Email Policy

Services provided by IT, which support the factory 24 hours a day, 7 days a week, 365 days a year include:

- Daily Change Control Reviews
- Security Administration and Auditing
- Computer and Network Operations
- Disaster Recovery and Business Continuity Planning
- Incident and Problem Management
- Physical Security Administration
- Tape Backup and Off-site storage

## **Data**

Market data received from our partners enters our secure systems via FTP, SFTP, Email, and PGP encrypted Email. Access to data is limited to authorized personnel in accordance with NPD's confidential client data process. Data is classified with different access levels and handlers attest to NPD's security policies before gaining access. Stewards of the data have hard disk encryption in use and data processing areas are secured using native file system protections from the supporting operating systems. Backups of client confidential data are also encrypted on tape.

NPD's data lies either in databases or in flat files. Database transactions are logged in the database and record counts audited for internal compliance.



*Behind Every Business Decision*

## **Obligations and Commitments of The NPD Group Information Technology Environment**

### External Access to NPD Data

The NPD Group, Inc. DecisionKey™ platform is provided to clients for the consumption of market research data as stipulated via the customer's standard services contract. Any user of DecisionKey™ will be provided a named ID by NPD which via a secure HTTP connection will grant them access rights to the data. The named user ID will be password protected and must not be shared with any other individual in the client organization or outside the organization. The password shall be kept secret and updated at regular intervals basis based on NPD's DecisionKey™ password parameters. Users of DecisionKey™ shall not distribute data to outside entities in any print, electronic, or other medium without NPD's prior written consent.

In receiving data from our retailer clients, NPD strongly recommends the use of secure transmission methods such as SFTP (Secure File Transmission Protocol) and email encryption (PGP or equivalents).

### Internal Access to NPD Data

Employees and contractors of The NPD Group, Inc. upon employment are required to read several policies with regards to Information Technology which define how security/data is handled at NPD. After reading the policies employees and contractors are asked to attest to the fact they have read and understand the policy. A record is kept by our Human Resources department. Changes to the policy are made periodically with any adjustments or addendums to the documents called out for the staff's review. The policies are available on the NPD Intranet for review at any time.

Employees and contractors are also classified with an internal security level clearance if the need to view client confidential data is required. Employee management submits a process document in which they receive additional training materials on how to handle confidential client data. The staff will also review any contractual agreements between NPD and its clients to ensure data are handled appropriately based on classification. Additional security processes are implemented using information technology products such as DLP (Data Loss Prevention) and WDE (Whole Disk Encryption) with limits applied to all removable media.