

 GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Policy and Procedure	
Title:	Managing Authorization, Access, and Control to Information Systems and Request for Network Access Form		
Policy #:	435	Pages:	15
Document Type:	Technology & Security Standards		
Effective Date:	August 16, 2012	Revision Date:	
POC for Changes:	Division of Information Technology		
References:	(1) Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, Privacy Rule and Security Rule. (2) Georgia Technology Authority (GTA) Enterprise Security Policy Authorization and Access Management (GTA PSG: SS-08-010.01) (3) Appropriate Use and Monitoring (GTA PSG: SS-08-001.01) (4) Federal Information Security Management Act (FISMA) Reference 4: Security Planning (5) FISMA References 4-Security Planning, 5-Personnel Security, 12-Awareness and Training, 15-Access Control, 17-Audit and Accountability (6) Policy and Procedure 419: Appropriate Use of Information Technology Resources		

I. Purpose

- A.** Provide the general framework of the policy and procedure utilized by the Department of Community Health (DCH) to control access to information and associated applications governing agency operations.
- B.** Clearly document information access control policy and procedures.
- C.** Avoid the negative consequences that result when information systems are compromised, which consequences may include:
 - 1. Exposure of personal or private information and subsequent harm to individuals;
 - 2. Unauthorized access to DCH's applications including unauthorized viewing, modifications, and copying of data;
 - 3. Sanctions; and
 - 4. Negative media attention.
- D.** Provide for the development of access controls required to protect state and agency information systems.

- E.** Mitigate the risk of threats or incidents involving current or former employees or contractors who intentionally exceed or misuse an authorized level of access to state software applications or access data in a manner that affects the security of DCH data, systems or daily business operations.
- F.** Outline managers' responsibilities and role in managing authorization, access to and control of DCH's systems and applications as outlined specifically and agreed to in DCH Information Technology User Agreement.
- G.** Establish access control requirements for DCH contractors and business owners, as well as vendors, sponsors, and business partners, in regards to their role and responsibilities, when access to DCH data and/or use of applications associated with DCH operations is authorized.
- H.** Reinforce the role of the business owner in providing adequate oversight of contractors' responsibilities specific to access control outlined in DCH contracts.
- I.** Ensure that valid business needs for access associated with DCH assignments continue to exist and that those needs are periodically reviewed and evaluated.
- J.** Assure compliance with all laws that require access controls procedures, including those identified as "References" in the header at the beginning of this document.

II. Policy

- A.** DCH information systems shall be used solely for appropriate agency purposes, or in accordance with DCH business associate agreements, data use agreements or data sharing agreements (together, "Data Agreements").
 - 1. DCH information systems shall not be accessed by anyone who does not need access to the system, or access to the information contained in the system, to perform the activities and fulfill the responsibilities associated with his or her employment or work relationship with DCH or to perform the activities described in a current Data Use Agreement. See Policy and Procedure 419: Appropriate Use of Information Technology Resources.
 - 2. Those authorized to grant or revoke access to DCH information are responsible for following applicable procedures to ensure that access is appropriately assigned and modified or terminated promptly.
 - 3. Those accepting confidential information on behalf of DCH shall ensure that the requirements related to the acceptance of that information are followed.
 - 4. Addressing the misuse of Department information and violations of IT Policy and Procedure 419 is of paramount importance to DCH and will be dealt with on a priority basis. Alleged violations of this policy will be investigated in

accordance with the appropriate legal requirements and DCH disciplinary procedures, and when appropriate, sanctions, including, but not limited to, dismissal, will be imposed.

- B.** Unless specifically designated as a public information system, access to any DCH information system or state network and its resources shall require the use of identification and authentication credentials in accordance with Policy and Procedure 419 and the terms of applicable contracts.
- C.** All contracts that involve access to DCH systems shall include the requirement that DCH's Division of Information Technology be notified (in accordance with DCH instructions) immediately (and, in no event, more than 1 business day) after any modification of the need for access, including change of access or termination of access. This applies to all DCH business owners, contractors, and vendors.
- D.** Access authorization shall follow the guidelines established by this policy and procedure.
- E.** Access authorization shall be documented, monitored and managed in accordance with agency security procedures.
- F.** DCH deploys Role Based Access Control measures which are based on an individual's assigned role and responsibilities.
- G.** Roles are assigned by the Supervisor/Manager based on a DCH Worker's function within the organization.
- H.** Supervisors/Managers are responsible for validating and communicating roles and access, where the level of access to be authorized is the lowest level required for users to meet their assigned DCH responsibilities.
- I.** Upon termination of work for DCH or reassignment of job responsibilities, a DCH Worker's user IDs and passwords shall be disabled or deleted in accordance with the DCH Information Security procedures.
- J.** Upon re-assignment of job responsibilities, an employee's access privileges shall be changed accordingly.

III. Scope

- A.** This policy establishes requirements for individuals regarding access to all DCH information, including the responsibilities of stewardship and accountability for DCH information needed in carrying out DCH's mission and/or conducting DCH business.

- B.** This policy refers to information systems that are used by DCH. Access control is required in order to comply with federal and state regulations and to safeguard the confidentiality, integrity and availability of sensitive and confidential information, including PHI.
- C.** This policy describes those procedures necessary for requesting, modifying and deleting user access to systems, applications and data covered by federal, state and all other applicable rules and regulations.
- D.** This policy applies to all who have access to DCH systems but whose access is not specified in a Business Associate Agreement or a Data Use Agreement.

IV. Roles and Responsibilities

- A.** Georgia Technology Authority (GTA): GTA manages access to the State's technology infrastructure and network services. GTA also controls some applications used by DCH. In addition, GTA manages administrative access to State managed systems. GTA is responsible for IT matters related to the State's contracting with outside third-parties for GETS functions.
- B.** Georgia Building Authority (GBA) manages the office space occupied by DCH and provides the physical security necessary to provide a secure office environment for people, equipment and information. GBA also manages the Building Access Request System, and physical access to the building.
- C.** DCH Offices, Management, and Staff
 - 1. Commissioner
 - a) Leads DCH and conveys the importance of information security to DCH management and staff.
 - b) Supervises the CIO and communicates with other State leaders and the Governor's Office to promote efficient and effective information security measures. The Commissioner has the final authority regarding the granting or termination of information access rights.
 - 2. Chief Information Officer (CIO)
 - a) Designates a senior agency Information Security Officer (ISO) who shall carry out the CIO's responsibilities for information security access control planning and implementation.
 - b) Provides guidance and oversight regarding all DCH information security policies, procedures, and access control safeguards to address identity and access management.
 - c) Oversees the identification, implementation, and assessment of security access controls throughout DCH's Technology Enterprise.
 - d) Ensures that personnel with responsibilities for system, network, and application security access controls are appropriately trained.

- e) Assists other senior DCH management with their responsibilities for system, network, and application access security.
 - f) Oversees the coordination of cross-platform security access controls for DCH.
 - g) Collaborates with the Executive Director of GTA and other State CIO's to address technology and security issues, policies, and standards.
3. Agency Information Security Officer [in the Division of Information Technology]
- a) Manages information security access control planning and implementation on behalf of the CIO.
 - b) Coordinates the development, review, and acceptance of security access controls with IT system owners, access security administration staff, and business owners or authorizing officials.
 - c) Coordinates the identification, implementation, and assessment of network, system, and application access security controls.
 - d) Plays an active role in developing and updating security access control policies, procedures, and standards and assesses the security impact.
 - e) Collaborates with the State Chief Information Security Officer and other State agency Information Security Officers to address Enterprise Security Access Control Policies, Procedures, and Standards and their impact on DCH business operations.
 - f) Provides oversight and guidance to security administration and operations staff regarding security access control policies, procedures, and standards.
 - g) Ensures that all DCH Workers receive training necessary for them to protect the confidentiality, integrity, availability, privacy and security of the information over which they have control, or to which they have access, as a result of their access to DCH information systems. See Policy and Procedure 419.
4. Access Control Coordinator/DCH Systems Administrator
- a) Sets and administers system-wide security access controls appropriate for the authority given to users in accordance with the attributes or privileges associated with authorized access.
 - b) Acts as the first step of security by creating user ID's and
 - c) Passwords to access networks, systems, and applications.
 - d) Is appointed by the CIO as the owner of the authorized network access control list and maintains a master file of all Network Access Request Forms, and manages the authorized access control list.
 - e) Acts as the primary point of contact to control settings and coordinate administrative changes for state-wide applications, including assigning permission for certain functions and access levels.

5. Inspector General

- a) Oversees the criminal background check process for all DCH employees.
- b) Coordinates with Director of Human Resources to ensure proper background checks for independent contractors and temporary staffing agency employees are complete before access to information systems is granted.
- c) Directs investigations related to violations of DCH information security policies and procedures, including access control procedures, and works with the HIPAA Privacy and Security Officer to recommend sanctions.
- d) Coordinates with the Attorney General and law enforcement when any information security incidents involve criminal behavior.

6. Chief Financial Officer (CFO)

The CFO is the primary authority for access by DCH staff to the PeopleSoft Financial System and related data. The CFO must approve the level of access to the Financial Systems before user IDs and passwords are created.

7. Contracts Administration

- a) Is responsible for ensuring that all contracts with business entities that have access to DCH information systems, or that operate information systems on behalf of DCH, include provisions requiring the maintenance and implementation of acceptable information security controls, including access controls.
- b) Ensures that such contracts incorporate access controls related to DCH information systems and provide penalties for failure to promptly inform DCH of a need for access changes.

8. HIPAA Privacy and Security Officer

Works with the CIO, Information Security Officer and Commissioner to revise DCH security controls as needed and ensure proper documentation in DCH policies and procedures.

- a) Works with the CIO, Information Security Officer and Director of Communications to promote compliance with HIPAA security regulations and ensure that all DCH workforce members receive regular security awareness training, including training on access controls.
- b) Works with the Director of Contracts Administration to clarify roles and responsibilities regarding HIPAA security compliance by business associates and develop contract language to address access controls.
- c) Works with the Director of Support Services to promote physical access controls, including physical security of information systems

through worksite audits and support of secure document storage/destruction practices.

- d) Works with the Inspector General to investigate violations of DCH information security procedures and recommends sanctions for such violations.

9. Office of Human Resources

- a) Is responsible for ensuring that DCH maintains documentation showing that all independent contractors and temporary staffing agency workers have been properly screened in accordance with policies and procedures for background checks.
- b) Maintains documentation that each member of the DCH workforce has access only to those information systems necessary to perform his/her work.
- c) Ensures that all new members of the DCH workforce receive Information Privacy and Security training approved by the Information Security Officer and the HIPAA Privacy and Security Officer, which includes training on access restrictions, before receiving access to DCH information systems.
- d) Ensures that all new members of the DCH workforce sign an acknowledgment of the DCH information security procedures.
- e) Maintains HIPAA training and acknowledgment forms for DCH employees, and ensures that such forms are provided to the HIPAA Privacy and Security Officer for all independent contractors and temporary staffing agency workers.
- f) Ensures that all supervisors are aware of their responsibility to approve information system access only as needed and change the access whenever a staff member's access requirements change.
- g) Ensures that the process for termination of employment includes termination of access to information systems.

10. Support Services

- a) Coordinates with GBA and GTA to ensure that physical access to DCH workspace and information systems storage is properly limited through badge access and other controls.
- b) Works with law enforcement to notify DCH staff members of threats to information system arising from break-ins and thefts.
- c) Coordinates with DCH and other State leaders to ensure that business continuity plans are current and appropriate.
- d) Supports security breach investigations.

11. Director of Vendor and Grantee Management

- a) Monitors compliance by vendors with information security provisions in service level agreements, including provisions related to access controls.
- b) Is responsible for including information security audits in the vendor management audit process.

12. Director of Procurement/Agency Procurement Officer (APO)

The Director of Procurement/APO is the primary authority for access to the PeopleSoft Team Georgia Marketplace (TGM) data by DCH staff. The APO must approve the level of access to the TGM system before a user ID and password is created for the employee.

13. System Administrators

- a) Are uniquely responsible for enabling users to manage a system or server.
- b) When appropriate, authorize users to define or alter user IDs, set security controls on a system or alter system components. These higher level privileges are restricted and controlled and may be extended to performing system support and maintenance activities if not assigned at the enterprise level.
- c) Authorize and manage users' access to systems (as listed in the Request for Network Access Form) with privileges defined by job function and role within DCH.
- d) Serve as the primary business owners for the application/platform system with authorization to perform job functions.
- e) Validate privileges annually and report updates to the DCH Access Control Coordinator, and performs updates to DCH account privileges after ensuring that proper authorization has been obtained.
- f) Retain revalidation results, evidence of completion and supporting communications for at least 6 years per HIPAA requirements, and define and manage access control requirements, including authorization processes and user ID and password rules for managed applications and systems.
- g) Maintain event/activity logs on all actions for each application under their control.
- h) Are primarily responsible for access to all DCH data closets. Entry for any other staff is strictly prohibited unless an emergency (e.g., fire or water damage) dictates otherwise.

14. Individual Users

- a) Defined as any user or network member that requires access to any State network, system, or application that accesses, transmits, receives, or stores electronic information.

- b) DCH Workers must comply with Policy and Procedure 419: Appropriate Use of Information Technology Resources, which includes policies and procedures related to access controls.
- c) User IDs and Passwords for DCH applications shall not be shared and individual accountability for the security of those user IDs and Passwords must be maintained.
- d) Authorized users are responsible for keeping all account authentication information in a secure place and not permitting any other person to use such accounts for any purpose.
- e) Authorized users shall take all necessary precautions to safeguard the confidentiality of associated Passwords and shall change Passwords when directed to comply with agency security procedures.
- f) Authorized users shall notify the ISO immediately if their user account is compromised and shall not use a user ID or Password belonging to someone else.
- g) Each user is accountable for all activity performed using their assigned user ID or Password.
- h) Authorized users acknowledge that when they are no longer employees of DCH, authorization to use their assigned account ID's will be terminated.

D. State of Georgia recognizes three (3) types of user accounts: Application Interface Account, User Account and Privileged Account. [Application Interface Accounts can be privileged, if technically required, but User Accounts may not. All User Accounts should have a named owner and follow the password policies of the State.]

1. Application Interface Account – Application Accounts are used to allow system services or applications to connect to a system. These accounts are not intended for general user access.
2. User Account – User Accounts are designed for use by general users without administrative or privileged account system access.
3. Privileged Account – Privileged Accounts enable a user to manage a system or software application. They may allow a user to define or alter user IDs and set the security access controls on a system or alter system components. Access to Privileged Accounts is not granted to the general user and shall be restricted and controlled.

V. Procedure

A. Manager/Supervisor/Business Owner shall:

1. Complete a Request for Network Access form (see Attachment A) to identify an individual DCH-authorized user who requires access to the State network

or a DCH computer system/application. This form is required for access request initiation, updates, and terminations.

2. Print and sign in the Manager Approval section to indicate approval for the access requested. Scan and send the completed form electronically to the DCH Access Control Coordinator.
3. Keep the form in a secure, on-site location (e.g., the user's personnel file held by the Manager/Supervisor, the business owner's contract file), readily available upon request.
4. Review the authorization access of computer system and software annually for DCH workers under his/her direct supervision to ensure that a business need still exists for the specific systems or application(s).
5. Review authorized access as users change job positions or work assignments (e.g., promotion, demotion, transfer, role change, or extended leave) to ensure that access is maintained or revoked, as appropriate.

B. Access Coordinator/Agency System Administrator shall:

1. Grant, change, or terminate access as specified on the Network Access form and notify the manager/supervisor/business owner when complete.
2. Forward requests for specific applications to the designated system administrator.
3. Modify or revoke access privileges when users are operating outside their assigned work privileges.
4. Revoke access privileges during a user's extended leave or when deemed appropriate by the Human Resources Office.
5. When notified by a Division Chief or Human Resources, request appropriate modification or termination of access privileges to information assets and data systems in accordance with the following:
 - a) When the user terminates employment with DCH or the need for access no longer exists, access shall be terminated.
 - b) After 90 days of logon inactivity to information systems or software applications.
 - c) When there is unauthorized or wrongful use or disclosure of information, access shall be terminated in accordance with DCH security policy and procedures.
 - d) Upon completion of a project or contract work, access shall be terminated and the application administrator shall be notified. A Request for Network Access Form must be submitted before access can be reinstated.

C. Access to Functions

1. Users shall be granted access only to the extent necessary to perform their job functions at DCH, or to perform the required job tasks described in a current Business Associate or Data Use Agreement. Access can be restricted to specific functions within some applications. Whenever the software allows, access should be as specific and limited as is feasible. Users should only have read or write access to the specific ePHI data required for performing their appropriate job function. In most cases, user access will fall into one of the following categories:
 - a) Administrator/Super-User; or Privileged Accounts
 - b) Regular or Normal User Accounts
2. The minimum access control requirement is a username and strong password. Every user at DCH must have a unique username and password. User account names shall not be shared. See Policy and Procedure 419.
 - a) *Role-based* access may be employed where it improves specificity of access. Role-based access allows end-users to access information and resources based on their role within the organization. Role-based access can apply to job categories or to groups of people or individuals.
 - b) The use of *anonymous user accounts* violates this policy and are strictly prohibited, unless where authorized by the Division of Information Technology for specific business purposes such as training systems. The use of anonymous user accounts that are able to access internal agency IT resources, including, but not limited to, PHI, is strictly prohibited unless specifically authorized in writing by the CIO. (See glossary for more information on anonymous accounts.)

D. Eligibility for Access

1. Upon receipt of a completed Request for Network Access form, the Access Control Coordinator may grant restricted information system or application access to users as specified in the network access form documentation.
2. Employees with job related requirements to access PHI data will receive accounts with the appropriate PHI access credentials.
3. Contractors/Temporary staffing agency employees providing support to specific DCH functions on a time-limited basis may be authorized to access specific applications for the duration of their work assignments.
4. Access shall only be granted to users whose status with DCH is current.

5. Whenever job responsibilities change, the supervisor shall review and determine the appropriate access and request the corresponding changes by using the Request for Network Access Form.
6. Upon a change of employment status where system/data access is no longer authorized (e.g., upon termination of employment) employee system account access shall be terminated immediately.

E. Access Determination

1. Determining the access to specific applications necessary for job functions and responsibilities requires determining which applications are required based on those functions and the corresponding data needed.
2. Authorized users will be granted specific system access privileges based on job responsibilities and a valid need-to-know basis. This may include both business continuity and disaster recovery job areas. This practice is intended to limit the damage that could result from accidents or errors, and to comply with information privacy and security laws.

F. Monitoring and Oversight

1. The Information Security Officer shall conduct periodic reviews to validate the appropriateness of user accounts and access privileges.
2. System Administrators shall review access requirements annually.
3. Supervisors shall review user access at least twice per year. Reviews can be accomplished during an employee's midyear and annual performance reviews to ensure that each user's access is appropriate.
4. System administrators shall review all user access periodically as a critical function of his/her responsibility to ensure that all users are in current status.
5. All system users consent to such monitoring and accept responsibility to preserve the confidentiality, integrity, and availability of information accessed. See Policy and Procedure 419.

G. Training and Access

1. All DCH employees shall complete HIPAA security training during their new hire orientation and during refresher training as designated by the HIPAA Privacy and Security Officer.
2. Regularly scheduled system activity reviews shall be conducted by System Administrators to ensure that the level of access to the system is appropriate.

VI. Policy and Procedure Revisions

The Chief Information Officer (or his designee) is responsible for reviewing, maintaining and updating this policy and procedure, the attached DCH Information Technology User Agreement, and Information Security training materials as necessary and appropriate.

VII. Supporting Documentation

PeopleSoft 8.9 HCM Security	Upon approval application is faxed to State Accounting Office, 200 Piedmont Avenue, Suite 1602 West Tower, and Atlanta, GA 30334. Fax # 404-463-5089.
HRM Query Access Request	Upon approval application is faxed to HRMS Phoenix Security, 200 Piedmont Avenue, Suite 1602 West Tower, and Atlanta, GA 30334. Fax # 404-651-5113.
PeopleSoft FN Financial 9.0	Forms can be faxed to 404-463-5089 Attn: Security or mail forms to: State Accounting Office, 200 Piedmont Avenue, Suite 1602 West Tower, Atlanta, GA 30334, Attention: Security

VIII. Glossary of Terms

Access Control Coordinator	The authority given to an individual by the assignment of attributes or privileges that are associated with access control systems and that are required for setting and administering system-wide security controls. Individual is designated by the Chief Information Officer.
Administrator/Super-User	Is a special user account used for system administration. Depending on the operating system, the actual name of this account might be: root, administrator or supervisor.
Agency Procurement Officer (APO)	Primary authority for access to the PeopleSoft Team Georgia Marketplace (TGM) data by DCH staff.
Anonymous accounts/authentication	Anonymous user account authentication gives users access to restricted data areas without prompting them for a system registered user name or password.
Contractor	An organization or individual that contracts with the Department to supply a needed service or skill set.
Data Use Agreement	An agreement or memorandum of understanding in which individuals other than DCH Workers receive access to a DCH information system for specified purposes. Such agreements include business associate agreements, data sharing agreements and data use agreements.
DCH Worker	A DCH Employee or an individual employed by an entity other than DCH who works regularly in DCH workspace "on assignment" with DCH (such as independent

	contractors and temporary staffing agency employees.)
Georgia Building Authority (GBA)	The State Authority that manages the property occupied by State agencies and provides the physical security necessary to provide a secure environment for people, equipment and information.
Georgia Technology Authority (GTA)	The State Authority that establishes information security standards and requirements for the State of Georgia.
HIPAA	Health Insurance Portability and Accountability Act, a US law designed to provide privacy and security standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.
IT Sabotage	Cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access to networks, systems, or data with the intention of harming a specific individual, the agency, the agency's data, systems, and/or daily operations.
Individually Identifiable Health Information	Information or data, including demographic information collected from an individual, that meets the following criteria (i) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (iii) that identifies the individual; or (iv) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Privileged Account	Accounts that enable a user to manage a system or server.
Protected Health Information (PHI)	Protected health information is defined in 45 CFR 160.103, and means Individually Identifiable Health Information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
Resource Access Control Facility (RACF)	Designed to provide improved security and controls what users can do on the operating system.
Role Based Access (RBAC)	An approach to restricting system access to authorized users. The primary rule for RBAC is as follows: Role assignment and authorization: A user shall be granted system access based on his/her assigned and authorized active role in DCH.

Security Planning	Requires organizations to have security controls in place or planned for their information systems and the rules of behavior for individuals accessing the information systems.
Application Interface Account (API)	Used to allow system services or applications to connect to a platform resource.
Theft Of Information	Cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access to networks, systems or data with the intention of stealing or modifying confidential or proprietary information for the organization.
Third Parties	Parties who contract with the DCH that administer applications, on the agency's behalf, that are covered by HIPAA security regulations or that represent significant financial risk to the DCH.
User Account	Defined as general users with non-privileged system access.

Approved by:	Date:
Commissioner 	8/17/12

Request for Network Access

User Please Read First: This Form indicates that the User below requires access to certain Department of Community Health applications, some of which contain sensitive and protected information. Managers must comply with DCH Policy and Procedure 435: Managing Authorization, Access and Control of Information Systems when granting and changing access. This completed, signed form must be submitted to the DCH Access Control Coordinator at clewis@dch.ga.gov with a copy to helpdesk@dch.ga.gov and a copy to the authorizing manager before access will be granted. A completed form, signed by the Manager approving access, must be maintained by the DCH Access Control Coordinator and by the authorizing Manager.

Instructions: Users may be employees of DCH, DCH workers on current assignment through a State-wide service contract, or employees of entities which which DCH has a current Data Agreement. Only one item marked with an asterisk should be completed. For each User there must be either an Employee ID or a Data Agreement # or a Staffing Contract #. An Authorizing Manager is a Manager designated in writing by a Division Chief as authorized to grant access to DCH Information systems.

Req Type	New	Termination	Modification	Annual	Other (please specify below)	Date Requested	Effective Date
"X" if applicable							
User Name				Supervisor Name			
Employer				Supervisor email			
Employee ID*				Data Agreement #*			
Title				Staffing Contract #*			
Function				Authorizing Manager			
Division				Mgr. email			
Unit				Mgr. Phone #			

Space Management

Location		Office#		Wkst#		Floor	
----------	--	---------	--	-------	--	-------	--

Physical Access Controls

Restrictions (x =restricted floor)	5	31	33	34	35	36	37	38	39	40	SF	SORH	Access Badge Issued	
------------------------------------	---	----	----	----	----	----	----	----	----	----	----	------	---------------------	--

Request for IT Equipment

New Order	Y/N	Issue Date	Ret. Date	Asset #1	Existing Equipment	Asset#
Desk Top (Y/N)					Desk Top (Y/N)	
Lap Top (Y/N)					Lap Top (Y/N)	
Blackberry (Y/N)					Blackberry (Y/N)	
Other (Y/N)					Other (specify)	

Note: New Users who receive IT Equipment receive standard software package: MS Office, Adobe Acrobat Reader, CITRIX, WinZip, Virus Scan, Internet Explorer, and MS Outlook. For additional software, use special software request area below.

Request for Access to DCH Applications

Admin Only	Read Only	Write/Edit	Remote	Applications	Admin Only	Read Only	Write/Edit	Remote	Applications	GETS Services: Expedite charges apply for short-interval service requests. AT&T to begin levying charges on MNS requests January 1, 2012 for all managed network service requests with due dates sooner than the standard interval for delivery of that service would permit.																																																
				Dataprobe					PeopleSoft	Managed Network Service Request <table border="1"> <thead> <tr> <th>Y/N</th> <th>Business Days</th> <th>Voice/Data Request</th> </tr> </thead> <tbody> <tr> <td></td> <td>7</td> <td>Centrex/Key (1-9 lines)</td> </tr> <tr> <td></td> <td>10</td> <td>Centrex/Key (10-19 lines)</td> </tr> <tr> <td></td> <td>10</td> <td>Centrex Phone 1-9 lines</td> </tr> <tr> <td></td> <td>15</td> <td>Centrex Phone 10-19 lines</td> </tr> <tr> <td></td> <td>7</td> <td>Email Add/Delete</td> </tr> <tr> <td></td> <td>5-7</td> <td>Feature Change Voice Line</td> </tr> <tr> <td></td> <td>3</td> <td>VM Password Reset</td> </tr> <tr> <td></td> <td>5-7</td> <td>VM Add/Delete Exist Line</td> </tr> <tr> <td></td> <td>5</td> <td>Toll FreeService (Simple)</td> </tr> <tr> <td></td> <td>5</td> <td>Audio/Web Conferencing</td> </tr> <tr> <td></td> <td>7</td> <td>VPN User ID</td> </tr> <tr> <td></td> <td>30</td> <td>Cplx Data Software Change</td> </tr> <tr> <td></td> <td>45</td> <td>Hardware (routers, switch)</td> </tr> <tr> <td></td> <td>15</td> <td>Add CRM Only</td> </tr> <tr> <td></td> <td>Varies</td> <td>Req for Solution</td> </tr> </tbody> </table>	Y/N	Business Days	Voice/Data Request		7	Centrex/Key (1-9 lines)		10	Centrex/Key (10-19 lines)		10	Centrex Phone 1-9 lines		15	Centrex Phone 10-19 lines		7	Email Add/Delete		5-7	Feature Change Voice Line		3	VM Password Reset		5-7	VM Add/Delete Exist Line		5	Toll FreeService (Simple)		5	Audio/Web Conferencing		7	VPN User ID		30	Cplx Data Software Change		45	Hardware (routers, switch)		15	Add CRM Only		Varies	Req for Solution
Y/N	Business Days	Voice/Data Request																																																								
	7	Centrex/Key (1-9 lines)																																																								
	10	Centrex/Key (10-19 lines)																																																								
	10	Centrex Phone 1-9 lines																																																								
	15	Centrex Phone 10-19 lines																																																								
	7	Email Add/Delete																																																								
	5-7	Feature Change Voice Line																																																								
	3	VM Password Reset																																																								
	5-7	VM Add/Delete Exist Line																																																								
	5	Toll FreeService (Simple)																																																								
	5	Audio/Web Conferencing																																																								
	7	VPN User ID																																																								
	30	Cplx Data Software Change																																																								
	45	Hardware (routers, switch)																																																								
	15	Add CRM Only																																																								
	Varies	Req for Solution																																																								
				CATS					Human Capital Management																																																	
				CRAM (Contract Reporting &Monitoring System)					Financial Services																																																	
				DFCS SUCCESS					Team Georgia Marketplace																																																	
				GAMMIS					Thompson Reuters																																																	
				GBA Badge Access					SharePoint																																																	
				ITRACE					Vendor Management																																																	
				Kronos					Grant Administration																																																	
				Laserfische					SABA (Learning Management)																																																	
				MEMS (SHBP)					Witness Call Reporting (SHBP)																																																	
				MEUPS					Unified Arts/Voice Mail																																																	
				G:Drive Restricted Folders					Other (Pls Specify)																																																	
				0:Drive Restricted Folders																																																						
				Budget																																																						
				HIPAA Privacy & Security																																																						
				Medical Policy (Medicaid Only)																																																						
				Other (Please Specify)																																																						
				PEHB Accounting																																																						
				Personnel																																																						
				S: Drive (SHBP Only)																																																						

Additional Notes (Requestor Only)

Authorizing Manager's Signature	Date
IT Department Use Only	