
Former Brunswick Naval Air Station
Designed for Nuclear Disaster


OXFORD NETWORKS
DATA CENTER
Please Ring Bell
on Door to
Your Right

IMG_1972.jpg

IMG_1973.jpg

IMG_1978.jpg

IMG_1980.jpg

IMG_1981.jpg

IMG_1983.jpg

IMG_1985.jpg

IMG_1987.jpg

IMG_1990.jpg

IMG_1992.jpg

IMG_2027.jpg

IMG_2028.jpg


OXFORD NETWORKS


NETGEAR
Room Alert
SONICWALL
PRO 2040
SONICWALL
PRO 2040
D-Link
NETGEAR


NETGEAR
Room Alert
SONICWALL
PRO 2040
SONICWALL
PRO 2040
D-Link
NETGEAR


TP-LINK
NETGEAR
D-Link
WAN
LAN
COLOVM2
COLOVM1
ABERDEEN


FIRE
WARNING
RESTRICTED AREA
KEEP OUT
AUTHORIZED PERSONNEL
ONLY
W149

OXFORD NETWORKS

www.oxfordnetworks.com

Oxford Data Center, LLC
491 Lisbon Street
Lewiston, ME 04240

01/21/2013

Dear Valued Clients:

Thank you for taking the time to review our attached Report on Controls at a Service Organization Relevant to Security, Availability and Confidentiality (SOC 2). This report was produced by Macpage LLC at my request and provides our clients an examination of the data center services we offer. Oxford Data Center, LLC is one of the first data center service providers among our industry peers to elect to have an SOC 2 examination performed.

Oxford Data Center, LLC elected to have a SOC 2 Type 1 examination performed to keep pace with our continued efforts to be an industry leader and demonstrate our leadership in the market place. Successful completion of the Audit indicates that Oxford Data Center, LLC processes, procedures and controls have been formally evaluated and tested. The examination included the company's controls related to security monitoring, change management, service delivery, support services, backup and environmental controls, logical and physical access.

The entire staff here at Oxford Data Center, LLC wishes to thank you and would like to take this opportunity to reaffirm our commitment to providing you the outstanding service and professionalism you expect from a business that cares about you and all our clients. Please be assured that we are all involved and continuously looking for ways to improve our company and further enhance our relationship with you.

Sincerely,

Craig S. Gunderson
President & CEO

INDEPENDENT SERVICE AUDITORS' REPORT

INDEPENDENT SERVICE AUDITORS' REPORT

TO THE BOARD OF DIRECTORS OF OXFORD DATA CENTER, LLC
LEWISTON, MAINE

SCOPE

We have examined the description in Section II of this report (description) and the suitability of the design of controls to meet the criteria for the security, availability, and confidentiality principle set forth Trust Services Principles (TSP) section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria), as of October 31, 2012.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Oxford Data Center, LLC's controls are suitably designed, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

SERVICE ORGANIZATION'S RESPONSIBILITIES

In Section II, Oxford Data Center, LLC has provided an assertion, which is based on the criteria identified in management's assertion. Oxford Data Center, LLC is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting controls to meet the applicable trust services criteria.

SERVICE AUDITORS' RESPONSIBILITIES

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Oxford Data Center, LLC's assertion and on the suitability of the design of the controls to meet the applicable trust service criteria, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed to meet the applicable trust services criteria as of October 31, 2012.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion theron.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

INHERENT LIMITATIONS

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

OPINION

In our opinion, in all material respects, based on the description criteria identified in Oxford Data Center, LLC's assertion in Section II and the applicable trust services criteria,

a. the description fairly presents the system that was designed and implemented as of October 31, 2012.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the control operated effectively as of October 31, 2012 and user entities applied the complementary user entity controls contemplated in the design of Oxford Data Center, LLC's controls as of October 31, 2012.

DESCRIPTION OF TESTS OF CONTROLS

The specific controls we tested and the results of our tests are presented in the section III of our report.

The information included in Sections I and IV of this report is presented by Oxford Data Center, LLC to provide additional information to user entities and is not a part of Oxford Data Center, LLC's description of its system and the suitability of the design of controls. The information in Sections I and IV has not been subjected to the procedures applied in the examination of the description of the controls, and the suitability of the design of controls to meet the applicable trust services criteria stated in the description, and accordingly, we express no opinion on it.

RESTRICTED USE

This report and the description of test of controls and results therof are intended solely for the information and use of Oxford Data Center, LLC; user entities of Oxford Data Center, LLC's Data Center Services as of October 31, 2012; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, or other parties;

- Internal control and its limitations;
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

South Portland, Maine
January 29, 2013

Common Census

IT Security Policy

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	July 25, 2012	Daniel Freund	Original
First Revision	May 17, 2013	Adrian Anghel	

Table of Contents

Common Census®

1. POLICY STATEMENT

"It shall be the responsibility of the I.T. Department to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized members of staff, and to ensure the integrity of all data and configuration controls."

➢ Summary of Main Security Policies

- Confidentiality of all data is to be maintained through discretionary and mandatory access controls, and wherever possible these access controls should meet with C2 class security functionality. Class C2 is a security rating established by the U.S. National Computer Security Center (NCSC) and granted to products that pass Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) tests. A C2 rating ensures the minimum allowable levels of confidence demanded for government agencies and offices and other organizations that process classified or secure information. TCSEC standards were established in the 1985 DoD document, Department of Defense Trusted Computer System Evaluation Criteria, known unofficially as the "Orange Book" (evaluation criteria for networks, the Trusted Network Interpretation is known as the "Red Book").
- Access to data on all laptop computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.
- Only authorized and licensed software may be installed, and installation may only be performed by I.T. Department staff.
- The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it are removed from the workstation or rented laptop immediately.
- Data may only be transferred in accordance with HIPAA standards
- All diskette drives and removable media from external sources must be virus checked before they are used within the Organization.
- Passwords must consist of a mixture of at least 8 alphanumeric characters, and must be changed every 90 days and must be unique.
- Workstation configurations may only be changed by I.T. Department staff.
- The physical security of computer equipment will conform to recognized loss prevention guidelines. Access to company property is monitored at all times or doors are locked requiring either a key and alarm code to enter or personal identification by staff of the party seeking entry.
- To prevent the loss of availability of I.T. resources industry standard appropriate measures are employed for backing up data, applications and the configurations of all workstations.
- A business continuity including disaster recovery plan is in place. We conduct biennial tests of our Home Office in Westbrook and our colocation site at Oxford Networks colocation facilities in Brunswick ME.

2. VIRUS PROTECTION

- The I.T. Department maintains up to date virus scanning software for the scanning and removal of suspected viruses.
- Corporate file-servers are protected with virus scanning software.
- Workstations are protected by virus scanning software.
- All workstation and server anti-virus software are regularly updated with the latest anti-virus patches by the I.T. Department.
- All systems are built from original wherever possible, clean master copies whose write protection has always been in place. Only original master copies are used until virus scanning has taken place.
- All demonstrations by vendors are run on their machines or a laptop rental not connected to our network and not the Organization's.
- New commercial software is scanned before it is installed.
- All removable media brought in to the Organization are scanned by the IT Department before they are used on site.
- To enable data to be recovered in the event of a virus outbreak regular backups are taken by the I.T. Department.
- Users are kept informed of current procedures and policies.
- Users are notified of virus incidents.
- Employees are accountable for any breaches of the Organization's anti-virus policies.
- Anti-virus policies and procedures are reviewed regularly.
- In the event of a possible virus infection the user must inform the I.T. Department immediately. The I.T. Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

3. PHYSICAL SECURITY OF EQUIPMENT

Physical Security of computer equipment will comply with the guidelines as detailed below.

➢ REQUIRED PHYSICAL SECURITY

- All doors are locked at all times unless personnel are attending the door.
- Exterior windows are locked before leaving and are checked by the last person out.
- Door alarms are installed on entry points to the office and report to a central alarm system.
- Motion alarms are installed and placed to detect unauthorized entry.
- Laptop preparation area and server room are locked by IT staff.

➢ Server Room

- Servers are housed in a locked purpose built room.
- The server room contains an adequate air conditioning system to provide a stable operating environment to reduce the risk of system crashes due to component failure. A thermal alarm is in place to warn of overheating.
- No water, rain water or drainage pipes should run within or above the server room to reduce the risk of flooding.
- Power points are raised from the floor to allow the smooth shutdown of computer systems in case of flooding.
- Battery backup and generator power is available to the server room to help protect the computer systems in the case of a mains power failure.
- Access to the server room is restricted to IT Department staff.
- All contractors working within the server room are to be supervised at all times and the It Department is to be notified of their presence and provided with details of all work to be carried out, at least 48 hours in advance of its commencement.

4. ACCESS CONTROL

- Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights are kept to a minimum at all times.
- Where possible no one person will have full rights to any system. The I.T. Department controls network/server passwords and system passwords are assigned by the system administrator in the end-user department.
- The system administrators are responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.
- Access to the network/servers and systems are by individual username and password.
- Network usernames and passwords are not shared by users.
- All users have an alphanumeric password of at least 8 characters.
- Passwords will expire every 90 days and must be unique.
- Intruder detection will be implemented where possible. The user account will be locked after 3 incorrect attempts.
- The I.T. Department is notified of all employees leaving the Organization's employment. The I.T. Department removes the employees' rights to all systems immediately (as they depart the building).
- Network/server supervisor passwords and system supervisor passwords are stored in a secure location in case of an emergency or disaster, for example a fire safe at Resilient Communications.
- Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.
- The Administrator username on Windows is changed from the default setting.
- Default passwords on SQL Server are changed after installation.
- File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and Files can rights to directories, files will be flagged as read only to prevent accidental deletion.

5. LAN Security

➢ Hubs & Switches

LAN equipment, hubs, bridges, repeaters, routers, switches are kept in secure hub rooms. Hub rooms are kept locked at all times. Access to hub rooms is restricted to I.T. Department staff only. Other staff and contractors requiring access to hub rooms will notify the I.T. Department in advance so that the necessary supervision can be arranged.

➢ Workstations

Users must logout of their workstations when they leave their workstation for any length of time. Alternatively Windows workstations may be locked.

➢ Wiring

- All network wiring will be fully documented.
- All unused network points are de-activated when not in use.
- Users must not place or store any item on top of network cabling.
- Redundant cabling schemes are used where possible.

➢ Monitoring Software

- The use of LAN analyzer and packet sniffing software is restricted to the I.T. Department.
- LAN analyzers and packet sniffers are securely locked up when not in use.
- Intrusion detection systems will implemented to detect unauthorized access to the network

➢ Servers

- All servers are kept securely under lock and key.
- Access to the system console and server disk/tape drives are restricted to authorized I.T. Department staff only.

➢ Electrical Security

- All servers are fitted with UPS's that also condition the power supply.

- All hubs, bridges, repeaters, routers, switches and other critical network equipment will also be fitted with UPS's.
- In the event of a main power failure, the UPS's will have sufficient power to keep the network and servers running until the generator takes over.
- Software is installed on all servers to implement an orderly shutdown in the event of a total power failure.
- All UPS's are tested annually.

➢ Inventory Management

- The I.T. Department maintains a full inventory of all computer equipment and software in use throughout the Company.
- Computer hardware and software audits are carried out periodically. These audits are used to track unauthorized copies of software and unauthorized changes to hardware and software configurations.

6. Server Specific Security

- The operating system are kept up to date and patched on a regular basis.
- Servers are checked daily for viruses.
- Servers are locked in a secure room.
- Where appropriate the server console features are activated.
- Remote management passwords are different to the Admin/Administrator/root password.
- Users possessing Admin/Administrator/root rights are limited to trained members of the I.T. Department staff only.
- Use of the Administrator/Root accounts is kept to a minimum.
- Assigning security equivalences that give one user the same access rights as another user are avoided where possible.
- Users access to data and applications are limited by the access control features.
- Intruder detection and lockout are enabled.
- The system auditing facilities are enabled.
- Users must logout or lock their workstations when they leave their workstation for any length of time.
- All accounts are assigned a password of a minimum of 8 characters.
- Users will change their passwords every 90 days.
- Unique passwords are used.
- The number of grace logins is limited to 3.
- Network login time restrictions are enforced preventing users from logging in to the network outside normal working hours.
- In certain areas users are restricted to logging in to specified workstations only.

7. Wide Area Network Security

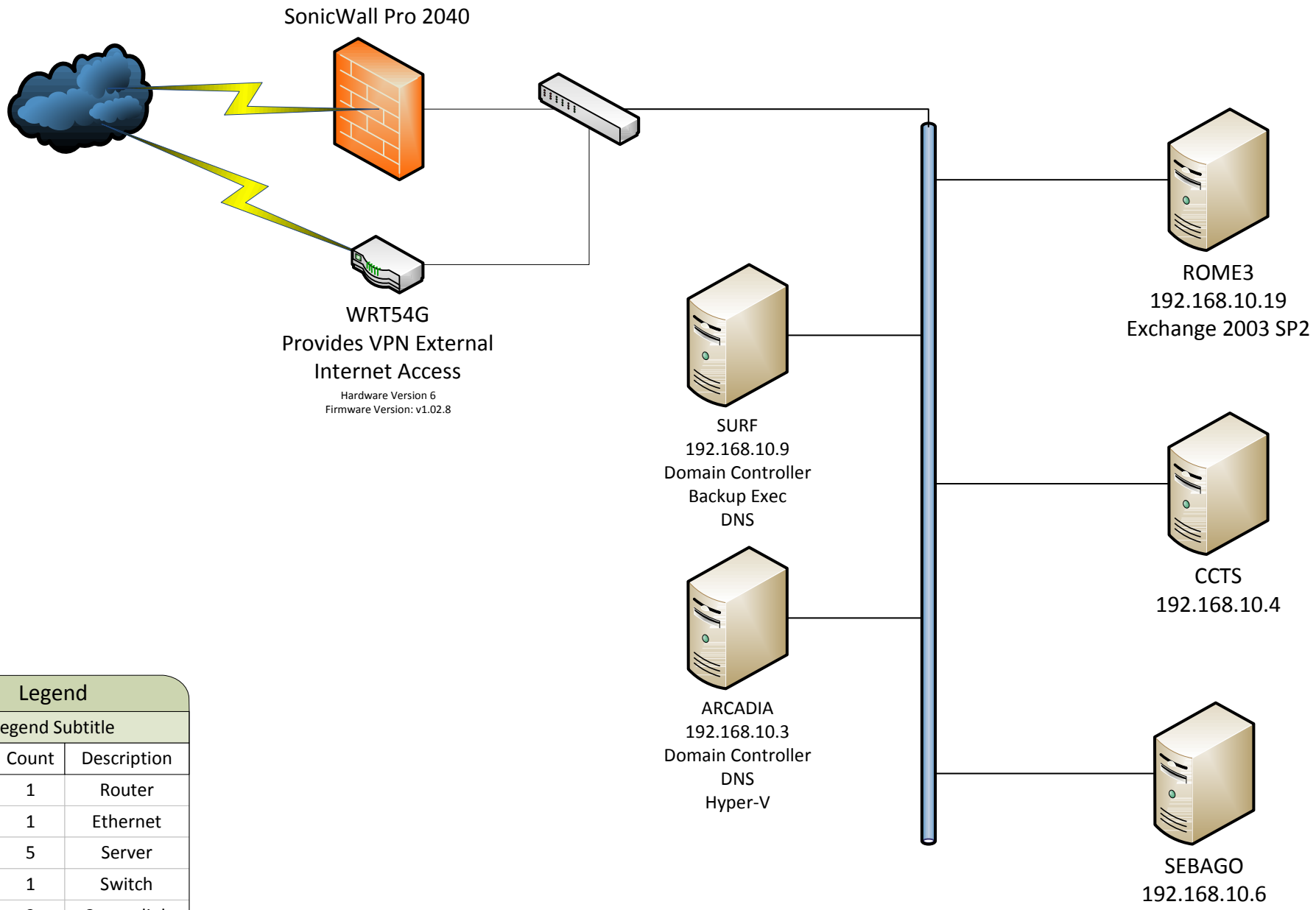
- Wireless LAN's will make use of the most secure encryption and authentication facilities available and it is also isolated from our production equipment (internet access is provided by a different ISP)
- Users will not install their own wireless equipment under any circumstances.
- A secure VPN tunnel is in place.
- Modems will not be used by users without first notifying the I.T. Department and obtaining their approval.
- Modems will only be used where necessary, in normal circumstances all communications should pass through the Organization's router and firewall.
- All bridges, routers and gateways are kept locked up in secure areas.
- Unnecessary protocols are removed from routers.
- The preferred method of connection to outside Organizations is by a secure VPN connection, using IPSEC or SSL.

8. TCP/IP & Internet Security

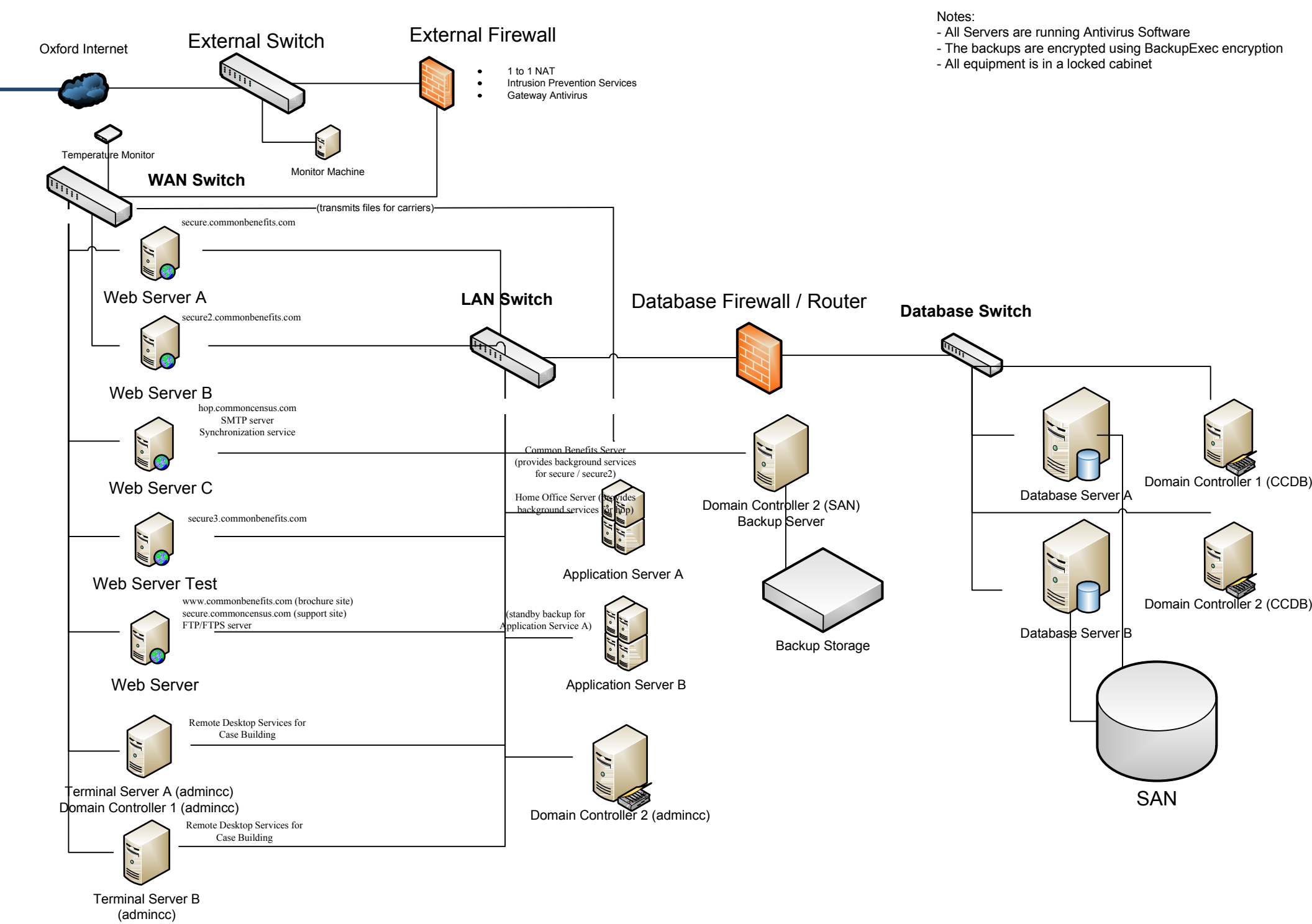
- Permanent connections to the Internet are via the means of a firewall to regulate network traffic.
- Permanent connections to other external networks, for offsite processing etc., are via the means of a firewall to regulate network traffic.
- Network equipment is configured to close inactive sessions.
- All incoming e-mails are scanned by the Organization's e-mail content scanner.

HQ Network Diagram

Updated: 5/14/2013

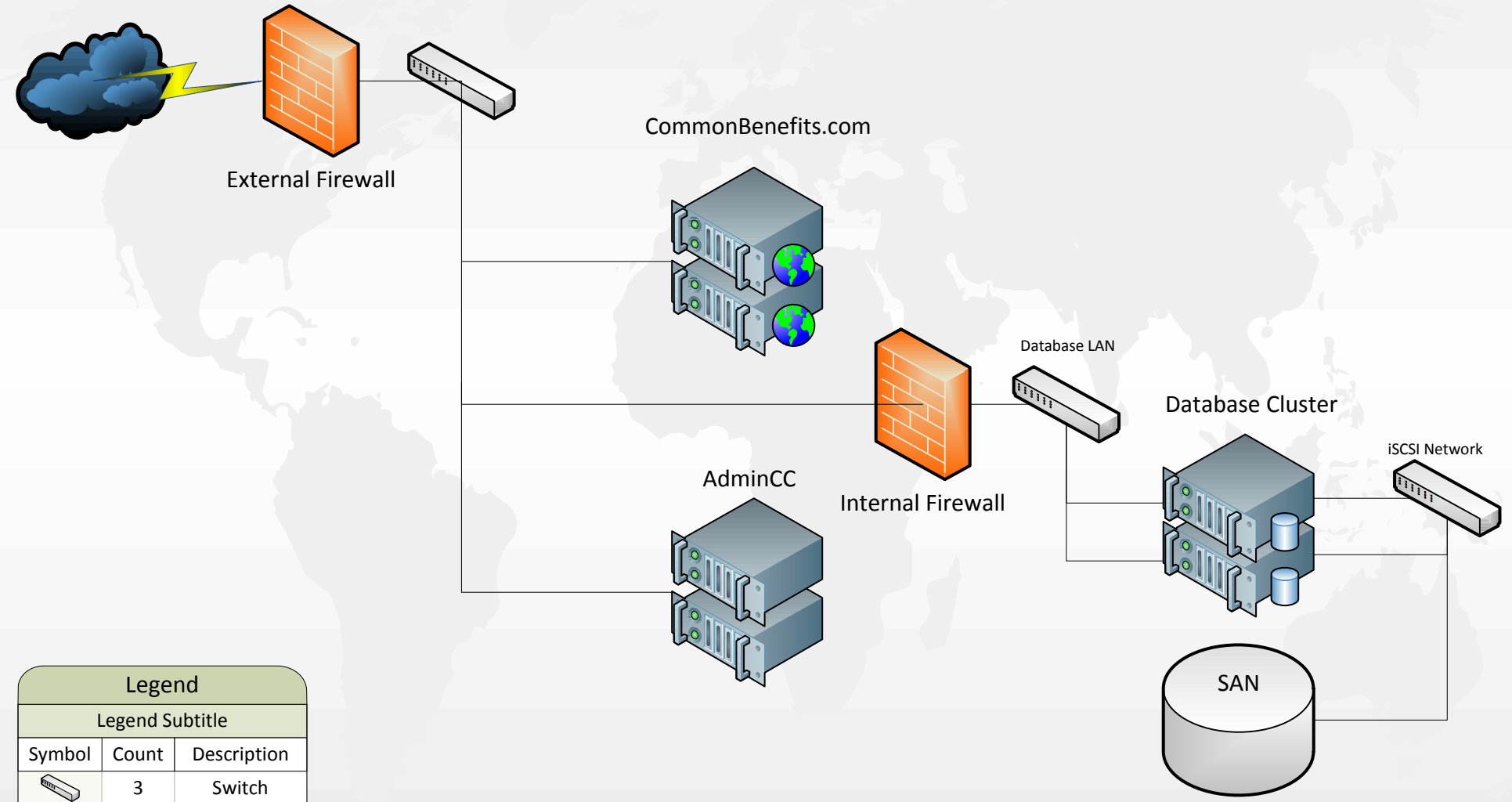


Legend		
Legend Subtitle		
Symbol	Count	Description
	1	Router
	1	Ethernet
	5	Server
	1	Switch
	2	Comm-link
	1	Cloud
	1	Firewall



Database Network Diagram

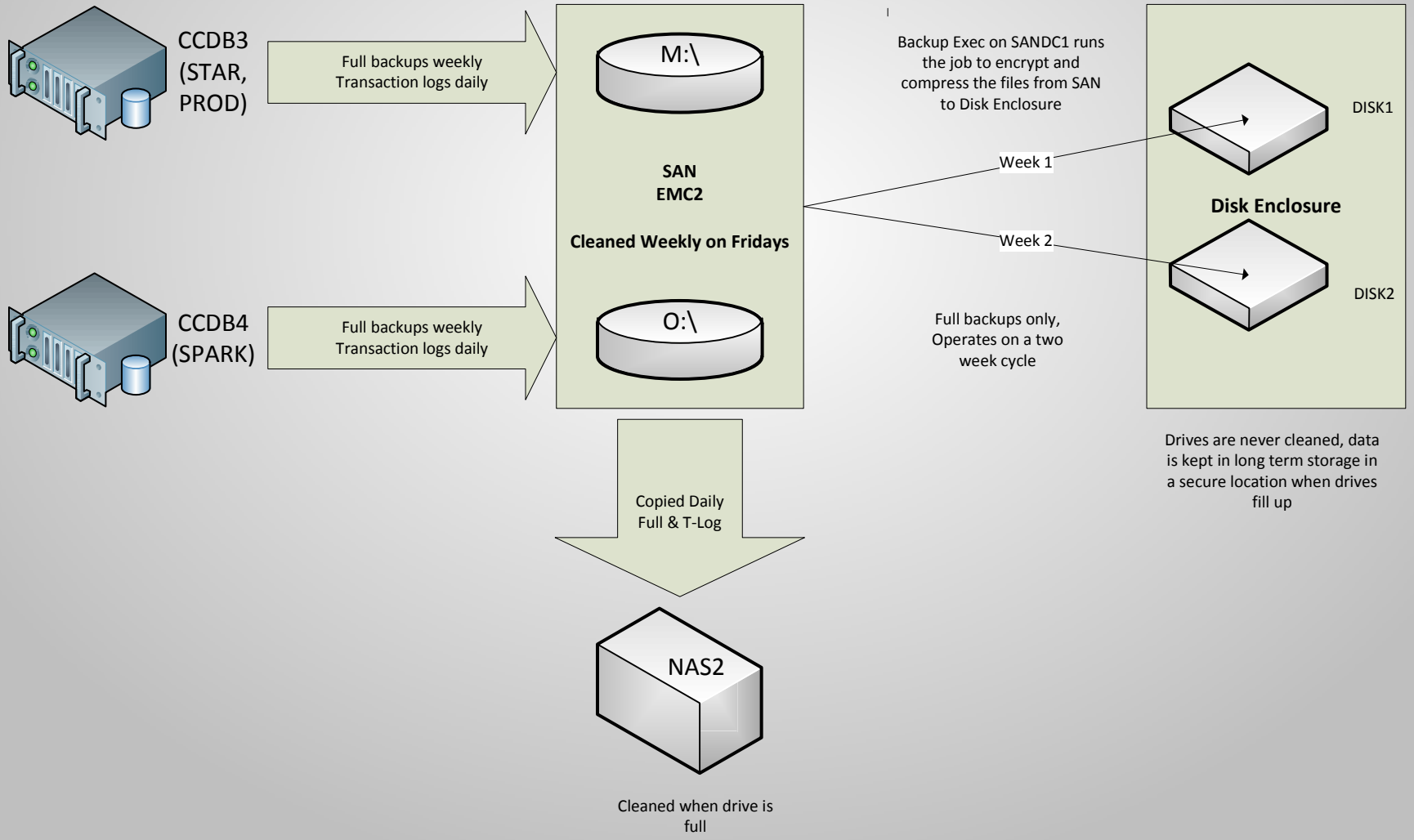
December 5, 2011



Legend		
Legend Subtitle		
Symbol	Count	Description
	3	Switch
	2	Firewall
	1	Data
	1	Internet
	1	Comm-link

Colo Database Backups

December 2, 2011



COMMON CENSUS SOFTWARE AND APPLICATION SERVER PROVIDER LICENSE

BEFORE YOU EITHER (1) INSTALL THE COMMON CENSUS EMPLOYEE BENEFITS SOFTWARE PRODUCT (THE "SOFTWARE") ON YOUR COMPUTER, OR (2) LOG ON TO THE COMMON CENSUS ASP EMPLOYEE BENEFITS SYSTEM (THE "SERVICE"), PLEASE CAREFULLY REVIEW ALL TERMS AND CONDITIONS OF THIS LICENSE (THE "LICENSE") AND BE SURE YOU UNDERSTAND THEM. BY CHOOSING "I ACCEPT" YOU BECOME A PARTY WITH COMMON CENSUS, INC. (HEREIN "COMMON CENSUS") TO THE LICENSE AND ARE LEGALLY BOUND BY ITS TERMS AND CONDITIONS AS SHOWN WHETHER YOU ARE AN INDIVIDUAL OR ENTITY. IF YOU DO NOT AGREE TO ANY OF THE TERMS AND CONDITIONS SHOWN, YOU MUST NOT INSTALL THE SOFTWARE OR LOG ON TO THE SERVICE. THE TERMS OF THIS AGREEMENT SUPERCEDE THE TERMS OF ANY PURCHASE ORDER THAT YOU MAY SUBMIT.
THIS AGREEMENT INCORPORATES THE TERMS AND CONDITIONS OF THE SUBSCRIPTION AGREEMENT FOR USE OF THE SOFTWARE AND SERVICE.

DATA MANAGEMENT DISCLAIMER
COMMON CENSUS AND COMMON BENEFITS TOOLS INVOLVE INFORMATION ACCUMULATED FROM THE EMPLOYER, THE INDIVIDUAL (EMPLOYEE), INSURANCE INTERMEDIARIES (BROKERS, CONSULTANTS) CARRIERS AND OTHER PARTIES THAT MAY USE THE DATABASE. THE INFORMATION FEED INTO THE DATABASE AND THE INFORMATION EXTRACTED FROM THE DATABASE IS ONLY AS ACCURATE AS THE PARTICIPANTS THAT ARE USING THE SYSTEM. FURTHERMORE, THE BUSINESS PROCESS OF SENDING DATA TO HOME OFFICES, THIRD PARTY ADMINISTRATORS OR OTHER ENTERPRISES THAT ARE EXPECTING DATA DELIVERY (ON A REGULAR OR AD HOC BASIS) IS CONTROLLED BY THE END USER. COMMON CENSUS WORKS WITH LICENSE HOLDER TO DEVELOP A PROCESS BUT IT IS THE RESPONSIBILITY OF THE LICENSEE TO EXERCISE THE TOOLS PROVIDED AND THE RESPONSIBILITY OF THE LICENSEE TO ASSURE DATA REACHES THE INTENDED DESTINATION.

BENEFITS INFORMATION DISCLAIMER.
THE SOFTWARE IS DESIGNED TO ASSIST AN EMPLOYER WITH THE ADMINISTRATION OF EMPLOYEE BENEFITS. IT IS NOT INTENDED, NOR MAY IT BE IN ANY MANNER CONSIDERED A SUBSTITUTE FOR SPECIFIC LEGAL OR TAX ADVICE ABOUT ANY BENEFIT,
QUALIFIED PLAN OR INSURANCE PROGRAM. TAX AND LEGAL MATTERS AS WELL AS ALL COMPLIANCE ISSUES MUST BE REVIEWED AND APPROVED BY YOUR OWN LEGAL OR TAX ADVISORS. ENROLLMENT, RATES, AND ADMINISTRATIVE OPERATIONS MUST BE CONFIRMED WITH EACH CARRIER.
OFFICIAL ENROLLMENT AND/OR CHANGES FOR ALL INSURANCE PRODUCTS MUST BE COMPLETED ON INSURANCE COMPANY APPROVED FORMS.
RECORDING OF DATA IN THIS PROGRAM MAY NOT BE SUFFICIENT TO SATISFY ANY CARRIER UNLESS SUCH CARRIER HAS SPECIFICALLY APPROVED IT.

GRANT OF LICENSE IN SOFTWARE AND SERVICE.

This License grants you the following rights to use the Software and Service, which is licensed to you and not sold:

- Application Server. You may access and use the Service running remotely on the server provided by Common Census (the "Site") according to the terms of the Subscription Agreement.
- Application Software. You may install the Software on one (1) CPU. You must periodically access the Site to validate the license for installed software.
- Database Backup. The Software and Service creates a database containing your employee benefit information (the "Database"), which is stored on a special server at the Site. Under this License, you may make and store an unlimited number of copies of the Database on a storage device of your choosing, such as a network server, with such copy to be used only to back up and re-install the database on the Site.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

- Limitations on Reverse Engineering, Decompilation, Disassembly and Access. You may not copy, reproduce, modify, reverse engineer, de-compile, or disassemble the Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. As per the terms of the Subscription Agreement, you agree

to notify CC immediately of any circumstances of which you have knowledge relating to any unauthorized use or copying of the Software or access to the Site by any persons or entity not authorized to do so.

- Separation of Components. The Software is licensed as a single product. Its component parts may not be separated for use on more than one computer.
- Rental. You may not rent or lease the Software or permit access to the Site to others.
- Software Transfer. You may permanently transfer all of your rights under this License, provided you retain no copies of the Software, you transfer all of the Software (including all component parts, the media and printed materials, any upgrades, this License and, if applicable, the Certificate of Authenticity), and the recipient agrees to the terms of this License. If the Software is an upgrade, any transfer must include all prior versions of the Software.
- Termination. Without prejudice to any other rights, Common Census may terminate this License if you fail to comply with the terms and conditions of this License and the Subscription Agreement. In such event, you must destroy all copies of the Software and all of its component parts.

COPYRIGHT.
All title and copyrights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Common Census. The Software is protected by U.S. copyright laws and international treaty provisions. Therefore, you must treat the Software like any other copyrighted material except that you may either make copies of the database solely for backup or archival purposes. You may not copy the printed materials accompanying the Software.

CONFIDENTIALITY AND SECURITY.

- Security. Common Census will take reasonable steps to keep your data stored on the Site private by (1) transmitting your data in encrypted form over a secure socket connection to the Site and (2) maintaining good security practices on the Site. You acknowledge that such security efforts by Common Census are reasonable under the circumstances. You further agree to use the same care and discretion to avoid disclosure, publication, or dissemination of your own data, but in no event less than reasonable care. You agree promptly to notify Common Census in writing of any circumstances that become known to you surrounding any possession, use, or knowledge of your data by any person or entity other than those authorized under this Agreement. You agree to assume sole responsibility for the security of your own hardware configuration and the passwords used in accessing the Site.
- Client System Requirements, Responsibilities. You are responsible for procuring, installing and maintaining at your location such hardware, software and Internet connectivity as may be required to run the Software and access the Site. Common Census reserves the right to charge additional service fees if you require assistance with respect to such basic setup.
- US Government Restricted Rights. The Software and documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) or the Commercial Computer Software--Restricted Rights at 48 CFR 52.227-19, as applicable.
  Manufacturer is Common Census, Inc., 90 Bridge Street 1st Floor, Westbrook, ME 04092.

MISCELLANEOUS.
This License is governed by the laws of the State of Maine and applicable U.S. law. In the event of a dispute between the parties, you irrevocably submit to the jurisdiction of the state or federal courts sitting in Maine, with venue in Cumberland County, Maine.

LIMITED WARRANTY.
Common Census warrants that the Software and the Service will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES.
Your exclusive remedy shall be, at Common Census' option, either (a) refund of the setup fees and subscription fees for the three (3) months prior to the event giving rise to a warranty issue, or (b) repair or replacement of the Software that does not meet Common Census' Limited Warranty and which is returned to Common Census. This Limited Warranty is void if failure of the Software or hardware has resulted from accident, abuse, or misapplication. Any replacement Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.
Outside the United States, neither these remedies nor any product support services offered by Common Census are available without proof of purchase from an authorized international source.

NO OTHER WARRANTIES.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, COMMON CENSUS DISCLAIMs ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, WITH REGARD TO THE SOFTWARE AND SERVICE. THIS LIMITED WARRANTY GIVES YOU SPECIFIED LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

EXPORT COMPLIANCE.
You hereby (1) assure Common Census that you shall adhere to the U.S. Export Administration laws and regulations and shall not export, re-export or release any software, source code, technical data, or products received from Common Census or the direct product of such software, source code or technical data to any proscribed country listed in the U.S. Export Administration regulations unless properly authorized by the U.S. Government, and (2) agree that this assurance will be honored even after expiration of this Agreement. You acknowledge that you are familiar with U.S. Government export policy and regulations and undertake to be and remain in full compliance with such policy and regulations.

LIMITATIONS OF LIABILITY.
COMMON CENSUS SHALL NOT BE HELD LIABLE FOR ANY DAMAGES SUFFERED, WHETHER IN CONTRACT, IN TORT, UNDER ANY WARRANTY THEORY, OR OTHERWISE FOR ANY AMOUNT IN EXCESS OF THE TOTAL AMOUNT PAID TO COMMON CENSUS BY YOU PURSUANT TO THIS AGREEMENT DURING THE THREE (3) MONTHS PREVIOUS TO THE EVENT CAUSING SUCH DAMAGES. UNDER NO CIRCUMSTANCES SHALL COMMON CENSUS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES (INCLUDING LOST PROFITS) OF A PARTY OR ANY THIRD PARTY, EVEN IF A PARTY HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, BUT WITHOUT LIMITATION, COMMON CENSUS SHALL HAVE NO LIABILITY FOR ANY LOSS, CORRUPTION, OR INACCURACY OF ANY OF YOUR DATA OR OF ANY OF YOUR CUSTOMERS OR THIRD PARTIES THAT MAY RESULT IN WHOLE OR IN PART FROM THE USE OF THE COMMON CENSUS SOFTWARE.

EXPORT COMPLIANCE.
You hereby (1) assure Common Census that you shall adhere to the U.S. Export Administration laws and regulations and shall not export, re-export or release any software, source code, technical data, or products received from Common Census or the direct product of such software, source code or technical data to any proscribed country listed in the U.S. Export Administration regulations unless properly authorized by the U.S. Government, and (2) agree that this assurance will be honored even after expiration of this Agreement. You acknowledge that you are familiar with U.S. Government export policy and regulations and undertake to be and remain in full compliance with such policy and regulations.

Common Census & Common Benefits HIPAA & GLBA

The Data Management Agreement (the "Agreement") between Common Census Inc. (CC) and the User is amended to include the following (i) American Recovery and Reinvestment Act of 2009 (the "ARRA"), (ii) Gramm-Leach-Bliley ACT ("GLBA") provisions, as required by regulations promulgated by state departments of insurance (the "GLBA Rules") and (iii) disclosure of compensation provisions:

A. HIPAA
In the event User has access to, receives, creates, transmits or maintains Protected Health Information, as defined below, in the course of performing duties under this Agreement, User shall be subject to the following terms and conditions:

1. Definitions. The following terms shall have the meaning set forth below:
(a) C.F.R. "C.F.R" means the Code of Federal Regulations.

(b) Designated Record Set. "Designated Record Set: has the meaning assigned to such term in 45 C.F.R. 164.501.

(c) Electronic Protected Health Information. "Electronic Protected Health Information" or "ePHI" means information that comes within paragraphs 1 (i) or 1 (ii) of the definition of "Protected Health Information", as defined in 45 C.F.R. 160.103.

(d) Individual. "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. 164.501 and shall include a person who qualifies as personal representative in accordance with 45 C.F.R. 164.502 (g).

(e) Protected Health Information. "Protected Health Information" or "PHI" shall have the same meaning as the term "Protected Health Information", as defined by C.F.R. 160.103, limited to the information created or received by User from or on behalf of Common Census.

(f) Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. 164.501.

(g) Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

(h) Secretary Incident. "Secretary Incident" shall have the same meaning as the term "security incident" in 45 C.F.R. 164.304.

(i) User. "User" means any individual who is accessing Common Census, Common Benefits, ND Enroller, or related technology.

2. Obligations of User
(a) User agrees to not use or disclose PHI other than is permitted or required by the Agreement or as Required By Law. User shall also comply with any further limitations on uses and disclosures agreed to by CC in accordance with 45 C.F.R. 164.522 provided that such agreed upon limitations have been communicated to User according with Section 4.1(c) of this Agreement.

(b) User agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement.

(c) User agrees to mitigate, to the extent practicable, any harmful effect that is known to User of a use or disclosure of PHI by User in violation of the requirements of this Agreement.

(d) User agrees to report to CC any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware.

(e) User agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by User on behalf of CC agrees to the same restrictions and conditions that apply through this Agreement to User with respect to such information. In no event shall User, without CC prior written approval, provide PHI received from, or created or received by User on behalf of CC, to any employee or agent, including a subcontractor, if such employee, agent or subcontractor receives, process or otherwise has access to the PHI outside of the United States. Subcontractor(s) who work for CC are subject to the same terms and conditions as CC.

(f) User agrees to provide access to CC, at the request of CC and in the time and manner designated by CC, to PHI in a Designated Record Set or, as directed by CC, to an Individual in order to meet the requirements under 45 C.F.R. 164.524. CC's determination of what constitutes "Protected Health Information" or a "Designated Record Set" shall be final and conclusive. If User provides copies or summaries of PHI to an Individual it may impose a reasonable, cost-based fee in accordance with 45 C.F.R. 164.524 (c)(4).

(g) User agrees to make any amendment(s) to PHI in a Designated Record Set that CC directs or agrees to pursuant to 45 C.F.R. 164.526 at the request of CC or an Individual, and in the time and manner designated by CC. User shall not charge any fee for fulfilling requests for amendment. CC's determination of what PHI is subject to amendment pursuant to 45 C.F.R. 164.526 shall be final and conclusive.

(h) User agrees to make (i) internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by User on behalf of CC, and (ii) policies, procedures and documentation relating to the safeguarding of ePHI available to the CC, or at the request of the CC to the Secretary, in a time and manner designated by the CC or the Secretary, for purposes of the Secretary determining CC's compliance with the Privacy and Security Rules.

(i) User agrees to document such disclosures of PHI as would be required for CC to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. 164.528.

(j) User agrees to provide to CC, in the time and manner designated by CC, the information collected in accordance with Section 2(i) of this Agreement, to permit CC to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. 164.528.

(k) User acknowledges that it shall request from CC and so disclose to its affiliates, subsidiaries, agents and subcontractors or other third parties, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.

(l) With respect to ePHI, User shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of CC, as required by 45 C.F.R. Part 164, Subpart C.

(m) With respect to ePHI, User shall ensure that any agent, including a subcontractor, to whom it provides ePHI, agrees to implement reasonable and appropriate safeguards to protect it.

(n) User shall report to CC any Security Incident of which it becomes aware.

3. Permitted Uses and Disclosures by User
3.1 General Use and Disclosure
Except as otherwise limited in this Agreement, User may use or disclose PHI to perform its obligations under this Agreement, provided that such use or disclosure would not violate the Privacy and Security Rules if done by CC or the minimum necessary policies and procedures of CC.

3.2 Specific Use and Disclosure Provisions
(a) Except as otherwise limited in this Agreement, User may use PHI for the proper management and administration of the User or to carry out the legal responsibilities of the User.

(b) Except as otherwise limited in this Agreement, User may disclose PHI for the proper management and administration of the User, provided that disclosures are Required By Law, or User obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the User of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this Agreement, User may use PHI to provide Data Aggregation services to CC as permitted by 45 C.F.R. 164.504(e)(2)(i)(B).

(d) User may use PHI to report violation of law to appropriate Federal and State authorities, consistent with 45 C.F.R. 164.502(j)(1).

4. Obligations of CC
4.1 Provisions for CC to Inform User of Privacy Practices and Restrictions
(a) CC shall notify User of any limitation(s) in CC's notice of privacy practices that CC produces in accordance with 45 C.F.R. 164.520 (as well as any changes to that notice), to the extent that such limitation(s) may affect User's use or disclosure of PHI.

(b) CC shall provide User with any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes affect User's use and disclosure of PHI.

(c) CC shall notify User of any restriction to the use or disclosure of PHI that CC has agreed to in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect User's use or disclosure of PHI.

4.2 Permissible Requests by CC
Except as may be set further in Section 3.2, CC shall not request User to use or disclose PHI in any manner that would not be permissible under the Privacy and Security Rules if done by CC.

5. Miscellaneous
(a) Regulatory References. A reference in this Agreement to a section in the Privacy and Security Rules means the section as in effect or as amended.

(b). Amendment. Upon the enactment of any law or regulation affecting the use or disclosure of PHI, the safeguarding of ePHI or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either party may, by written notice to the other party, amend this Agreement in such manner as such party determines necessary to comply with such law or regulation. If the other party disagrees with such amendment, it shall so notify the first party in writing within

thirty (30) days of the notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, then either of the parties may terminate the Agreement on thirty (30) days written notice to the other party.

(c) Interpretation. Any ambiguity in this Agreement shall be resolved to permit CC to comply with the Privacy and Security Rules.

(d) Effective six (6) months after the issuance of applicable final regulations pursuant to the ARRA of 2009, Common Census shall not directly or indirectly receive remuneration in exchange for any PHI without a valid authorization permitting such remuneration, except as permitted by law.

(e) This Agreement shall be construed and enforced in accordance with the laws of the State of Maine.

B. GLBA
In the event User maintains, processes, or otherwise is permitted access to customer information, as defined below, in the course of performing duties under this Agreement, User shall be subject to the following terms and conditions:

6. Definitions. The following terms shall have the meanings set forth below:
(a) Customer Information. "Customer Information" means nonpublic personal financial and health information about a customer, whether in paper, electronic or other form. Customer Information includes any such information provided by the customer as part of a request for information about, or an application for, a CC insurance product or service. Even if no such insurance product or service is subsequently provided to the customer.

7. Obligations of User.
(a)User agrees to implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of Customer Information that are appropriate to User's size, complexity, nature and scope of activities, and that is designed to:

(i) ensure the integrity and confidentiality of Customer Information;

(ii) protect against any anticipated threats or hazards to the security or integrity of Customer Information; and

(iii) protect against unauthorized access to, or use of, Customer Information that could result in substantial harm or inconvenience to any customer.

(b) User agrees to ensure that any agent, including a subcontractor, to whom it provides Customer Information received from, or created or received by User on behalf of CC, agrees to the same restrictions and conditions that apply through this Agreement to User with respect to such Customer Information.

(c) In no event shall User, without CC's prior written approval, provide Customer Information (received from, or created or received by User on behalf of CC) to any employee or agent, including a subcontractor, if such employee, agent or subcontractor receives, processes, or otherwise has access to the Customer Information outside of the United States. Any foreign worker(s) that is allowed access to PHI is subject to the same terms and conditions as the CC staff.

(d) User agrees to make policies, procedures, and documentation relating to the safeguarding of Customer Information available to CC, or at the request of CC to the applicable department

COMMON CENSUS GENERAL POLICY STATEMENT

The policy of Common Census, Inc., (“We”, “Us” or “Common Census”) is to respect and protect the privacy and confidentiality of the information conveyed to Common Census by employers, brokers and agents who use Common Census services, software and Internet tools. We will take such commercially reasonable actions as may be required under the circumstances to preserve the confidentiality of any information a client identifies as being proprietary and confidential in nature.

By its nature, employee benefits administration requires confidential employee data. This includes employee contact information (e.g. name, address, email), unique identifiers (e.g. social security number, employee ID), dependent information (e.g. names and ages of a spouse and children), financial information (e.g. income, insurance limits, account numbers, the cost of benefit elections), and demographic data (e.g. zip code, age, income). Common Census and the employer define the source and update protocol for each data element. Common Census intends to collect, retain, and disclose Personal Information only on a "need to know" basis.

Vendor Privacy Policies.

The insurers, financial service providers and other providers and suppliers of goods and services who are represented by Common Census and/or with whom our Producers may transact business using Common Census software and Internet Sites (collectively, the “Vendors”) will have privacy policies in effect from time to time that are applicable to, and intended for the benefit of, the ultimate purchasers of the products and services offered or supported through Common Census and the Producers (“Vendor Privacy Policies”). Common Census will use commercially reasonable efforts to convey the Vendor Privacy Policies to the Producers.

Aggregate Statistics.

Common Census gains the consent of the employer or employee prior to using information in any manner other than defined below, and prior to knowingly disclosing Personal Information to a third party. Common Census uses Personal Information to:

- Administer and / or market the benefits program to providers (e.g. insurance carriers) as authorized by the employer;
- Aggregate Data;
- Generate reports authorized by the employer; and
- Provide services an employee requests.

Data Security

Confidentiality is a major concern with any online system. Accordingly, several precautions have been taken to ensure that information is kept protected at all times. All information sent to and from Common Census Internet applications is encrypted using a combination of 40-bit secured socket layer (SSL) technology, digital certificates, and firewalls. These security features work together to provide users with a mutually authenticated communications path. Mutual authentication helps to ensure that only legitimate users can access the system, and that legitimate users see only the information they are intended to see.

Cookies and IP Addresses

A cookie is a small file, stored on your hard disk, sent to your browser from a web server. Common Census uses cookies to track your web session as you use the site, and the process of logging off deletes the cookie. Common Census uses the cookie to be sure your data goes to your PC, not somewhere else. Common Census does not put extraneous data in a cookie, and does not attempt to read other cookies on your PC. The website may provide erratic results if you choose to disable cookies on your browser. It is your responsibility to log off the Common Census site when you have finished using it, to delete the cookie from the PC after each user session. Employers, Insurance brokers/agents or Employees may choose to transmit Personal Information to websites controlled, owned, or operated by third parties, including insurance carriers. In this situation, the privacy statements of those third parties govern their use of this information, not this Privacy Statement. Account Access and Passwords Each registered user of Common Census Internet Tools and software will be assigned a password in order to access that user’s account and account information. It is the user’s responsibility to protect and preserve the confidentiality of the user’s password. Common Census will not be responsible for any loss resulting from unauthorized access to a user’s account.

A PASSWORD SHOULD NEVER BE GIVEN TO ANY PERSON WHO THE REGISTERED USER HAS NOT AUTHORIZED TO TRANSACT BUSINESS ON THE USER’S BEHALF USING THE SITE RESOURCES.

ANY PERSON WHO IS GIVEN A USER’S PASSWORD WILL HAVE ACCESS TO ALL OF THE USER’S

INFORMATION THAT IS STORED ON THE SITE AND MAY HAVE THE ABILITY TO CHANGE OR DELETE THAT INFORMATION.

No Resale of Information

Common Census never resells, trades, leases or rents the personally identifiable information of our users to other companies.

Common Census Home Office
Westbrook

Business Continuation Policy & Disaster Recovery Plan (DRP)

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	August 12, 2012	Adrian Anghel & Dale Darling	Original
	May 22, 2013	Adrian Anghel & Dale Darling	First Revision
	June 26, 2013	Dale Darling	Second Revision

Common Census®

Table of Contents

Common Census®

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

➢ Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

➢ Objectives

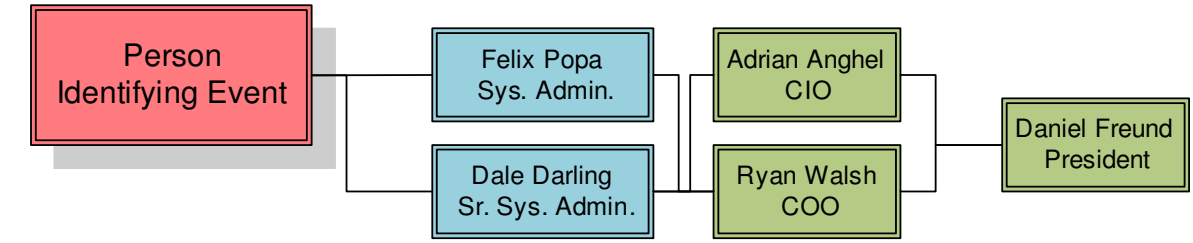
The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Describe disaster recovery capabilities as applicable to key customers, vendors and others

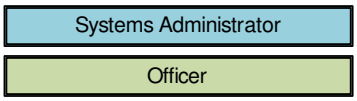
➢ Key Personnel Contact Info[DF1]

Role	Company	Individual	Phone	Email
Landlord	Dana Mill	Peter Cook	207-712-3036	PeterGCookEsq@aol.com
Property Manager	Boulos	Greg McKellar	207-871-1290	gmckellar@boulos.com
Colocation	Oxford Networks	Support	207-837-6899	support@oxfordnetworks.com
Colocation	Oxford Networks	Michael L. Tompkins	(207) 333-3460	mtompkins@oxfordnetworks.com

➢ Notification Calling Tree



Legend:



Chain of Command:

1. **President**
2. **CIO, COO**
3. **Senior Systems Administrator**
4. **Systems Administrator**

➢ External Contacts[DF2]

Colocation	Oxford Networks	Support	207-837-6899	support@oxfordnetworks.com
Colocation	Oxford Networks	Michael L. Tompkins	(207) 333-3460	mtompkins@oxfordnetworks.com

Plan Overview

➢ Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials.

This plan is reviewed and updated biennially or when events that significantly affect its effectiveness occur (i.e. personnel changes, equipment changes, environment changes etc.)

Last Update	June 2013
Next Scheduled Update	May 2015

➢ Plan Documentation Storage

It is necessary for the DRP documentation to be protected but in the same time accessible to the ERT in the event of a disaster.

- Master Copy of this plan is stored J:\IT Files\Disaster Recovery\Headquarters Disaster Recovery Plan.docx
- A copy of this plan and the associated documents in electronic format has been provided to the following people:

Daniel Freund (President)	June 26, 2013
Adrian Anghel (CIO)	June 26, 2013
Ryan Walsh (COO)	June 26, 2013
Dale Darling (Systems Administrator)	June 26, 2013
Felix Popa (Systems Administrator)	June 26, 2013

A printed copy is at Oxford Networks in our safe with backup materials.

➢ 1.3 Recovery Strategy

Key business processes and the agreed recovery strategy for each are listed below. The strategy chosen is a full restoration at a recovery site. This strategy entails recreating the production environment at the same or a different location (based on disaster category) in an expeditious manner.

KEY BUSINESS PROCESS	BACKUP STRATEGY
Email Services	Full restoration at recovery site
IT Operations	Full restoration at recovery site
PDS Services	Full restoration at recovery site

Development Services	Full restoration at recovery site
Phone System	Full restoration at recovery site
Finance	Full restoration at recovery site
Human Resources	Full restoration at recovery site

➢ 1.4 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We considered a wide range of potential threats and the results of our deliberations are included in this section. Numerous potential environmental disaster or emergency situation has been examined. The focus of our DRP is to limit the level of business disruption which could arise from each type of disaster and ensure the business continuity.

- Definition of disaster

For the purpose of this document we consider disaster a singular event or a group of events, natural or man-made, that render our services non-functional for an undetermined period of time or more than 12 hours.

- Disaster Categories

To attain the objectives described above we have grouped the disasters in two major categories and the second one in two subcategories:

Disaster Category 1 (D1)

Description: Services are down and our team doesn't have physical access to the HQ offices to correct the situation.

- **D1.1** People can work remotely
- **D1.2** People cannot work remotely

Disaster Category 2 (D2)

Description: Services are down and we have physical access to the colocation facility.

- **D2.1** Services are down due to external factors (i.e. power failure, internet connection down, etc.)
- **D2.2** Services are down due to equipment failure (i.e. equipment flooded, firewall failure, etc.)

Each category of disaster has an associated recovery plan.

Emergency Response

➢ Alert, escalation and plan invocation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

➢ Plan Triggering Events

There are a lot of circumstances that can lead to the activation of the DRP. We list here some key trigger issues at the colocation that would lead to activation of the DRP (the list is not all inclusive):

- Total loss of communication
- Total loss of power
- Flooding of the premises
- Fire on the premises
- Loss of equipment (theft, vandalism etc.)
- Loss of the building

➢ Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated immediately. The ERT will then decide the extent to which the DRP must be invoked.

The person discovering the incident calls a member of the Emergency Response Team in the order listed below:

Dale Darling	207-329-9348	dale.darling@commoncensus.com
Felix Popa	207-450-7571	felix.popa@commoncensus.com
Adrian Anghel	207-332-1634	adrian.anghel@commoncensus.com

If not available try:

• Ryan Walsh 207-712-3770

• Daniel Freund 207-450-7397

This ERT contact information will be made available to all our partners and all our customers when the DFP is deployed.

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

➢ Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 6.0 business hours
- Restore key services within 12.0 business hours of the incident
- Recover to business as usual within 16.0 to 24.0 hours after the incident
- Coordinate activities with disaster recovery team, first responders, etc.
- Notify internal personnel and external clients
- Report to the emergency response team.

➢ Alternate Recovery Facilities

We will use the Common Census Headquarters located in Westbrook Maine as the alternate recovery facility.

➢ Communications Protocol

- Privacy / Security / Accountability

Communication between team members during the emergency response has to follow the same privacy and security protocols that are in place during normal business process.

All written communications issued during the emergency response must be preserved in this path in Outlook: Public Folders/Common Census/Disaster Recovery/[disaster name]

- Personnel Notification

The COO will contact the manager of PDS who will call his staff. COO will contact the office manager who will notify all other staff of the DRP implementation.

- Clients Notification

PDS staff will notify their assigned clients via telephone. COO will notify all Home Office clients vial telephone.

Media

- President or COO will draft a media statement if needed
- Web announcements: An announcement will be posted at all relevant websites (Common Census, Common Benefits, Home Office Portals) when the websites become available.

Insurance

As part of the company's disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include errors and omissions, general liability, and business interruption insurance. The COO or President will deal with our insurance agent about relevant coverage.

Financial and Legal Issues

➢ Financial

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment includes:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

➢ Legal Issues

The President and ERT will jointly review the aftermath of the incident and after consulting the Board of Directors decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

Annual DRP Testing

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

The scenarios will be reviewed annually during the first quarter of every year.

Appendix A: Technology Disaster Recovery Plans

➢ Disaster Recovery Plan for Disaster Category 1 (D1)

Services	Email Services
Disaster Description	Email Services are down
Recovery Strategy	Disaster Categories D1 or D2.2 The alternate email server will be brought online at the colocation facility in Brunswick and all email will be redirected there. After that, a new Exchange server will be configured on the colo equipment, mailboxes and folders will be restored. Disaster Categories D2.1 The alternate email server will be brought online at the colocation facility in Brunswick and all email will be redirected there. After that, the equipment supporting the email services from the HQ will be moved to the colocation facility and reconfigured.
Associated Servers	*Local Domain* SURF (Domain Controller) ROME3 (Exchange Server) *CCENSUS Domain (at the colo) will be Restored* SURF (Equivalent Domain Controller) – RESTORED ROME3 (Equivalent Exchange Server) - RESTORED

KEY CONTACTS	
	Dale Darling 207-329-9348
	Felix Popa 207-450-7571
	Adrian Anghel 207-332-1634

➢ Resources:

	Source	
Mailboxes Backups	LTO-2 Tape; Full and Daily Incremental Backups stored off-site in Vault.	To find correct inventory, see "Backup_Inventory.xls"
Server Backups	Tape; Full and Daily Incremental Backups stored off-site.	To find correct inventory, see "Backup_Inventory.xls"
Disaster Recovery Site	Common Census Collocation Facility	
Restore Hardware	DR Tape drive already at COLO	DR Server Hardware already at COLO
Restore Software	Windows 2003 Server, Exchange 2003 Server	
Alternate Mail Server	POP Mail Server on SANDC1	
Mailboxes Backups	LTO-2 Tape; Full and Daily Incremental Backups stored off-site in Vault.	To find correct inventory, see "Backup_Inventory.xls"

➢ DR Steps for Disaster Categories D1 or D2.2:

1) Start the Alternate mail server service at COLO on SANDC1.
2) Modify DNS for mail.commoncensus.com to point to Public IP for SANDC1.
3) Add ALLOW access rule to COLO Firewall to allow incoming mail traffic (SMTP) and POP (for users to check mail) to alternate mail server.
4) Test incoming/outgoing mail accounts via external 3rd party mail service.
5) Test email server from inside and outside of the firewall.
6) Convey user credentials and connection information to CC Staff.
7) DR Laptops at COLO already have an installed email client and are ready for use. Configure laptops for CC Staff.
8) Begin restoration of CCENSUS DC to DR Server Hardware.
9) Install Windows 2003 on DR Server Hardware in to alternate directory (SEE Symantec TECH10797 – see support documentation for details on this "Disaster recovery of a local Windows 2003 computer"- included in support documents.)

10) Install backup/restore software and/or remote agent on DR Server Hardware
11) Inventory the backup tape media in BEWS.
12) Click Restore in BEWS.
13) Click General Settings, select the following: Choose to Restore all information for files and directories; Preserve Tree; Restore over existing files
14) Click Advanced Settings, select "Mark this server as the primary arbitrator for replication when restoring folders managed by the File Replication Service, or when restoring SYSVOL in System State."
15) Click Run Now to start the restore.
16) Reboot the computer after the restore has finished.
17) Physically connect the restored server to its own dedicated temporary network which is firewalled from the rest of the COLO infrastructure.
18) Begin restoration of Exchange server to DR Server Hardware. (SEE Symantec TECH10797 – see support documentation for details on this "Disaster recovery of a local Windows 2003 computer"- included in support documents.)
19) Install Windows 2003 on DR Server Hardware in to alternate directory.
20) Install backup/restore software and/or remote agent on DR Server Hardware
21) Inventory the backup tape media in BEWS.
22) Click Restore in BEWS.
23) Click General Settings, select the following: Choose to Restore all information for files and directories; Preserve Tree; Restore over existing files.
24) Begin restoration of Exchange by following instructions in the included support document: TECH20523 "How to restore Exchange 2000 or 2003 to a recovery server in a different forest".
25) After Exchange restoration is complete and no mount errors are reported, CC Staff may now connect to the Exchange Server, locally.
26) Disable Alternate Mail Server.
27) Configure firewall to direct incoming mail.commoncensus.com mail and POP requests to the restored Exchange Server.

➢ DR Steps for Disaster Categories D2.1:

1) Start the Alternate mail server service at COLO on SANDC1.
2) Modify DNS for mail.commoncensus.com to point to Public IP for SANDC1.
3) Add ALLOW access rule to COLO Firewall to allow incoming mail traffic (SMTP) and POP (for users to check mail) to alternate mail server.
4) Test incoming/outgoing mail accounts via external 3rd party mail service.
5) Test email server from inside and outside of the firewall.
6) Convey user credentials and connection information to CC Staff.
7) DR Laptops at COLO already have an installed email client and are ready for use. Configure laptops for CC Staff.
8) Configure HQ firewall with public IP assigned for DR purposes.
9) Connect all HQ servers to the physical network as they were at HQ. See HQ Network diagram included in support documents.
10) Connect DR Laptops as if they were HQ computers per the HQ Network diagram.

➢ Disaster Recovery Plan for PDS

Services	PDS Services
Disaster Description	PDS Department cannot perform their functions at the HQ Offices.
Recovery Strategy	Most of the functions performed by the PDS department are web enabled and can be performed remotely by connecting to the colocation systems. In the event of a disaster preventing the PDS department performing their duty at the HQ, people are instructed to connect to the colo and work remotely. If that is not possible, they can assemble and work at the colocation facility in space provided by Oxford Networks according to our existing agreement.
Associated Servers	*N/A*

KEY CONTACTS	
	Dale Darling 207-329-9348
	Felix Popa 207-450-7571
	Adrian Anghel 207-332-1634

KEY CONTACTS	
Hardware Vendor	Aberdeen Inc. Tim Jacobs 800-500-9526 x154
System Owners	Common Census, Inc.
Database Owner	Common Census, Inc.
Application Owners	Common Census, Inc.
Software Vendors	PC Connection, Ryan Allaire, 800-800-0014 x76380, 800-397-0650 Direct
Offsite Storage	Common Census, Inc.

RESOURCES		
GoDaddy Account Information	See same section of document "Disaster Recovery Plan Details.docx"	
IP Addresses Allocation	See same section of document "Disaster Recovery Plan Details.docx"	Document describing the IP addresses in use is at the colocation with the matching IP addresses reserved for the recovery site

DR Steps:

1) Change nameserver IPs at GoDaddy.com with new DR (Disaster Recovery) IPs – This may take minutes to hours to replicate so it's first to do – May take up to 24 hours with current DNS settings.
2) BEFORE disconnecting any network cabling, DOCUMENT the physical network connections.
3) If lack of power was not the cause of this DRP being put in to place, SHUTDOWN Services and Servers "nicely" based on power-down schedule.
4) Physically relocate all production hardware to DR site WITH EMPHASIS on deploying, plug-for-plug, switch-for-switch, the physical Network configuration as it was at the failed site.
5) Configure firewall with same one-to-one NAT but use DR IPs.
6) Update DNS Zone files on DR DNS server with new IPs
7) Power up Services and Servers using the power-up schedule.
8) Start and test Services one by one using Section 1.3 as a service list

➢ Disaster Recovery Plan for Disaster Category 2.2 (D2.2)

Services	All
Disaster Description	Services are down due to equipment failure (i.e. equipment flooded, firewall failure, etc.)
Recovery Strategy	Production hardware will be replaced as needed, reconfigured and brought online.
Associated Servers	Varies by failed equipment. To be identified at disaster time
Applications	Varies. Only services affected by failed equipment.

KEY CONTACTS	
Hardware Vendor	Aberdeen Inc. Tim Jacobs 800-500-9526 x154
System Owners	Common Census, Inc.
Database Owner	Common Census, Inc.
Application Owners	Common Census, Inc.
Software Vendors	PC Connection, Ryan Allaire, 800-800-0014 x76380, 800-397-0650 Direct
Offsite Storage	Common Census, Inc.

BACKUP STRATEGY	
Daily	Daily Transaction Logs; Weekly Full Backups (Data)
Monthly	Full Server Backup (non-data)
Quarterly	SEE Monthly and Daily above

DR Steps:

1) Identify failed unit or component.
2) Stop and Power off related services and servers using power-down schedule.
3) Replace failed component.
4) Power up Services and Servers using the power-up schedule.
5) Start and test affected Services one by one using Section 1.3 as a service list

Appendix B: Recovery Report

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management
-

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the BCP and lessons learned
- Lessons learned

Common Census Colocation Facility

Disaster Recovery Plan (DRP)

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	August 12, 2012	Adrian Anghel & Dale Darling	Original
	June 26, 2013	Dale Darling	Revision 1

Common Census®

Table of Contents

Common Census®

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

➢ Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

➢ Objectives

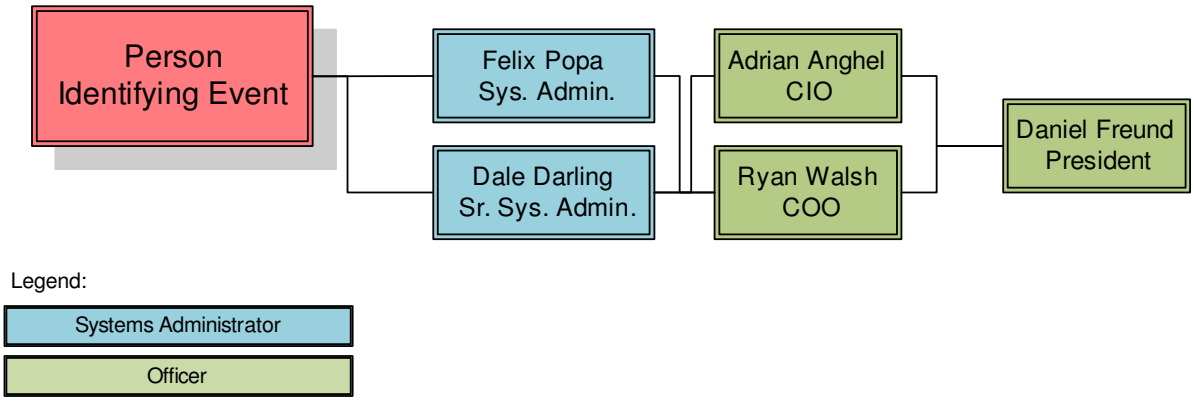
The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Describe disaster recovery capabilities as applicable to key customers, vendors and others

➢ Key Personnel Contact Info

Name	Title	Work Phone	Cell Phone	email
Dale Darling	System Administrator	207-854-5454 X212	207-329-9348	dale.darling@commoncensus.com
Felix Popa	System Administrator	207-854-5454 X222	207-450-7517	felix.popa@commoncensus.com
Adrian Anghel	CIO	207-854-5454 X210	207-332-1634	adrian.anghel@commoncensus.com
Daniel Freund	President	207-854-5454 X203	207-450-7397	daniel.freund@commoncensus.com
Ryan Walsh	COO	207-854-5454 X209	207-712-3770	ryan.walsh@commoncensus.com
Oxford Networks	Support	207-837-6899		

➢ Notification Calling Tree



Chain of Command:

1. **President**
2. **CIO, COO**
3. **Senior Systems Administrator**
4. **Systems Administrator**

➢ External Contacts

Role	Company	Individual	Phone	Email
Landlord	Dana Mill	Peter Cook	207-712-3036	PeterGCookEsq@aol.com
Property Manager	Boulos	Greg McKellar	207-871-1290	gmckellar@boulos.com
Colocation	Oxford Networks	Support	207-837-6899	support@oxfordnetworks.com
Colocation	Oxford Networks	Michael L. Tompkins	(207) 333-3460	mtompkins@oxfordnetworks.com

Plan Overview

➢ Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials.

This plan is reviewed and updated yearly or when events that significantly affect its effectiveness occur (i.e. personnel changes, equipment changes, environment changes etc.)

Last Update	June 26, 2013
Next Scheduled Update	May 2015

➢ Plan Documentation Storage

It is necessary for the DRP documentation to be protected but in the same time accessible to the ERT in the event of a disaster.

- Master Copy of this plan is stored J:\IT Files\Disaster Recovery\Colocation Disaster Recovery Plan.docx
- A copy of this plan and the associated documents in electronic format has been provided to the following people:

Daniel Freund (President)	June 26, 2013
Adrian Anghel (CIO)	June 26, 2013
Ryan Walsh (COO)	June 26, 2013
Dale Darling (Systems Administrator)	June 26, 2013
Felix Popa (Systems Administrator)	June 26, 2013

A printed copy is at Oxford Networks in our safe with backup materials.

➢ 1.3 Recovery Strategy

Key business processes and the agreed recovery strategy for each are listed below. The strategy chosen is a full restoration at a recovery site. This strategy entails recreating the production environment at the same or a different location (based on disaster category) in an expeditious manner.

KEY BUSINESS PROCESS	BACKUP STRATEGY
Common Benefits Administrators	Full restoration at recovery site
Common Benefits Groups	Full restoration at recovery site
Common Benefits Individuals	Full restoration at recovery site
Common Benefits Portal	Full restoration at recovery site

Home Office Portal	Full restoration at recovery site
Synchronization Service	Full restoration at recovery site
Common Census Public Website	Full restoration at recovery site
Common Census Support Website	Full restoration at recovery site
Admincc.com Terminal Services	Full restoration at recovery site

➢ 1.4 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We considered a wide range of potential threats and the results of our deliberations are included in this section. Numerous potential environmental disaster or emergency situation has been examined. The focus of our DRP is to limit the level of business disruption which could arise from each type of disaster and ensure the business continuity.

- Definition of disaster

For the purpose of this document we consider disaster a singular event or a group of events, natural or man-made, that render our services non-functional for an undetermined period of time or more than 12 hours.

- Disaster Categories

To attain the objectives described above we have grouped the disasters in two major categories and the second one in two subcategories:

Disaster Category 1 (D1)

Description: Services are down and our team doesn't have physical access to the colocation facility to correct the situation.

Disaster Category 2 (D2)

Description: Services are down and we have physical access to the colocation facility.

- **D2.1** Services are down due to external factors (i.e. power failure, internet connection down, etc.)
- **D2.2** Services are down due to equipment failure (i.e. equipment flooded, firewall failure, etc.)

Each category of disaster has an associated recovery plan.

Emergency Response

➢ Alert, escalation and plan invocation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

➢ Plan Triggering Events

There are a lot of circumstances that can lead to the activation of the DRP. We list here some key trigger issues at the colocation that would lead to activation of the DRP (the list is not all inclusive):

- Total loss of communication
- Total loss of power
- Flooding of the premises
- Fire on the premises
- Loss of equipment (theft, vandalism etc.)
- Loss of the building

➢ Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated immediately. The ERT will then decide the extent to which the DRP must be invoked.

The person discovering the incident calls a member of the Emergency Response Team in the order listed below:

Dale Darling	207-329-9348	dale.darling@commoncensus.com
Felix Popa	207-450-7648	felix.popa@commoncensus.com
Adrian Anghel	207-332-1634	adrian.anghel@commoncensus.com

If not available try:

• Ryan Walsh 207-712-3770

• Daniel Freund 207-450-7397

This ERT contact information will be made available to all our partners and all our customers when the DFP is deployed.

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

➢ Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 6.0 business hours
- Restore key services within 12.0 business hours of the incident
- Recover to business as usual within 16.0 to 24.0 hours after the incident
- Coordinate activities with disaster recovery team, first responders, etc.
- Notify internal personnel and external clients
- Report to the emergency response team.

➢ Alternate Recovery Facilities

We will use the Common Census Headquarters located in Westbrook Maine as the alternate recovery facility.

➢ Communications Protocol

- Privacy / Security / Accountability

Communication between team members during the emergency response has to follow the same privacy and security protocols that are in place during normal business process.

All written communications issued during the emergency response must be preserved in this path in Outlook: Public Folders/Common Census/Disaster Recovery/[disaster name]

- Personnel Notification

The COO will contact the manager of PDS who will call his staff. COO will contact the office manager who will notify all other staff of the DRP implementation.

- Clients Notification

PDS staff will notify their assigned clients via telephone. COO will notify all Home Office clients vial telephone.

Media

- President or COO will draft a media statement if needed
- Web announcements: An announcement will be posted at all relevant websites (Common Census, Common Benefits, Home Office Portals) when the websites become available.

Insurance

As part of the company's disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include errors and omissions, general liability, and business interruption insurance. The COO or President will deal with our insurance agent about relevant coverage.

Financial and Legal Issues

➢ Financial

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment includes:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

➢ Legal Issues

The President and ERT will jointly review the aftermath of the incident and after consulting the Board of Directors decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

Annual DRP Testing

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

The scenarios will be reviewed annually during the first quarter of every year.

Appendix A: Technology Disaster Recovery Plans

➢ Disaster Recovery Plan for Disaster Category 1 (D1)

Services	All
Disaster Description	Services are down and our team doesn't have physical access to the colocation facility to correct the situation
Recovery Strategy	All production services will be restored at the disaster recovery site using backups of the virtual machines for the systems and a backup database server.
Associated Servers	*SAN Domain, Public Facing* SANDC2 (domain controller) SANVDC (domain controller) CCWS3 (web server) CCWS4 (web server) CBWS4 (web server) CBWS5 (web server) CBWS6 (web server) CCAS1 (application server) CCAS2 (application server) CCTS5 (terminal server) CCTS6 (terminal server) *CCDB Domain, Private* CCDBDC1 CCDBDC2 CCDB5 CCDB6

KEY CONTACTS	
	Dale Darling 207-329-9348
	Felix Popa 207-450-7571
	Adrian Anghel 207-332-1634

Common Census®

Resources:

	Source	
Virtual Machines Backups	Most Recent VM Backup Disk – Located at HQ IN SRV RM disk storage shelf	
Database Backups	Most Recent DB Backup Disk – Located at HQ in SRV RM disk storage shelf	
Virtual Machines Host	One VMWare server with specifications matching the existing CCVM1 or CCVM2 machines is standing by if needed.	
Backup Database Server	CCDB3	
Backup Firewall	Existing Firewall at the HQ	For the list of firewall access rules, see "Colocation Disaster Recovery Firewall Config.txt".
GoDaddy.com Account Information	See same section of document "Disaster Recovery Plan Details.docx"	
IP Addresses Allocation	See same section of document "Disaster Recovery Plan Details.docx"	

DR Steps:

1) Change nameserver IPs at GoDaddy.com with new DR (Disaster Recovery) IPs – This may take minutes to hours to replicate so it's first to do – May take up to 24 hours with current DNS settings.
2) Identify the latest backups of the VM, restore to DR VM.
3) Start Backup Database Server SQL 2008 R2 DR server to receive database backups.
4) Restore Latest DB backups on SQL 2008 R2 DR.
5) Configure DR firewall with same one-to-one NAT but use DR IPs.
6) Update DNS Zone files on DR DNS server with new IPs.
7) Update database aliases on all restored servers so database Instance names point to new SQL server DR IP.
8) Confirm SQL server instance names resolve to correct IP on DR servers.
9) Start and test Services one by one in the following order:

   A. SANDC2 (domain controller)
   B. CBWS6 (secure3.commonbenefits.com)
   C. CCAS2
   D. CCWS3
   E. CBWS4
   F. CBWS5
   G. CCWS4
   H. CCAS1
   I. CCTS5
   J. CCTS6

➢ Disaster Recovery Plan for Disaster Category 2.1 (D2.1)

Services	All
Disaster Description	Services are down due to external factors (i.e. power failure, internet connection down, etc.)
Recovery Strategy	All production hardware will be relocated to DR site, reconfigured and brought online.
Associated Servers	*SAN Domain, Public Facing* SANDC2 (domain controller) SANVDC (domain controller) CCWS3 (web server) CCWS4 (web server) CBWS4 (web server) CBWS5 (web server) CBWS6 (web server) CCAS1 (application server) CCAS2 (application server) CCTS5 (terminal server) CCTS6 (terminal server) *CCDB Domain, Private* CCDBDC1 CCDBDC2 CCDB5 CCDB6

KEY CONTACTS	
	Dale Darling 207-329-9348
	Felix Popa 207-450-7571
	Adrian Anghel 207-332-1634

KEY CONTACTS	
Hardware Vendor	Aberdeen Inc. Tim Jacobs 800-500-9526 x154
System Owners	Common Census, Inc.
Database Owner	Common Census, Inc.
Application Owners	Common Census, Inc.
Software Vendors	PC Connection, Ryan Allaire, 800-800-0014 x76380, 800-397-0650 Direct
Offsite Storage	Common Census, Inc.

RESOURCES		
GoDaddy Account Information	See same section of document "Disaster Recovery Plan Details.docx"	
IP Addresses Allocation	See same section of document "Disaster Recovery Plan Details.docx"	Document describing the IP addresses in use at the colocation with the matching IP addresses reserved for the recovery site

DR Steps:

1) Change nameserver IPs at GoDaddy.com with new DR (Disaster Recovery) IPs – This may take minutes to hours to replicate so it's first to do – May take up to 24 hours with current DNS settings.
2) BEFORE disconnecting any network cabling, DOCUMENT the physical network connections.
3) If lack of power was not the cause of this DRP being put in to place, SHUTDOWN Services and Servers "nicely" based on power-down schedule.
4) Physically relocate all production hardware to DR site WITH EMPHASIS on deploying, plug-for-plug, switch-for-switch, the physical Network configuration as it was at the failed site.
5) Configure firewall with same one-to-one NAT but use DR IPs.
6) Update DNS Zone files on DR DNS server with new IPs
7) Power up Services and Servers using the power-up schedule.
8) Start and test Services one by one using Section 1.3 as a service list

➢ Disaster Recovery Plan for Disaster Category 2.2 (D2.2)

Services	All
Disaster Description	Services are down due to equipment failure (i.e. equipment flooded, firewall failure, etc.)
Recovery Strategy	Production hardware will be replaced as needed, reconfigured and brought online.
Associated Servers	Varies by failed equipment. To be identified at disaster time
Applications	Varies. Only services affected by failed equipment.

KEY CONTACTS	
Hardware Vendor	Aberdeen Inc. Tim Jacobs 800-500-9526 x154
System Owners	Common Census, Inc.
Database Owner	Common Census, Inc.
Application Owners	Common Census, Inc.
Software Vendors	PC Connection, Ryan Allaire, 800-800-0014 x76380, 800-397-0650 Direct
Offsite Storage	Common Census, Inc.

BACKUP STRATEGY	
Daily	Daily Transaction Logs; Weekly Full Backups (Data)
Monthly	Full Server Backup (non-data)
Quarterly	SEE Monthly and Daily above

DR Steps:

1) Identify failed unit or component.
2) Stop and Power off related services and servers using power-down schedule.
3) Replace failed component.
4) Power up Services and Servers using the power-up schedule.
5) Start and test affected Services one by one using Section 1.3 as a service list

Appendix B: Recovery Report

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management
-

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the BCP and lessons learned
- Lessons learned

_____

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management *(If different than completion date)*	

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name: _____

Signature: _____

Date: _____

(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)

I confirm that above business process is now acceptable for normal working conditions.

Name: _____

Title: _____

Signature: _____

Date: _____

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management *(If different than completion date)*	

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name: _____

Signature: _____

Date: _____

(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)

I confirm that above business process is now acceptable for normal working conditions.

Name: _____

Title: _____

Signature: _____

Date: _____