ENTERPRISE
information services

Disaster Recovery Planning

Kathleen Silva, Business Continuity Manager with Enterprise Information Services

**** DOCUMENT CLASSIFICATION NOTICE ****

The information in this document, while not confidential, is sensitive in nature. All distribution and discussion of this Enterprise Information Services plan is under the authority of the State Chief Information Officer, or any individual authorized to grant permission on their behalf. Functional plans that outline specific emergency response operations and procedures are exempt from Public Records Law in accordance with Oregon Revised Statutes 192.311 to 192.513.

- About Us
- Q&A
- Best Practices
- Disaster Recovery Planning
- Lessons Learned
- EIS Website

About EIS Data Center Services

- Tier 3 data center
  - Everything here is N+1 where N is the number of units needed to run something.
  - 16,000 sq ft regulated environment the data center sits on a raised floor that is monitored for heat and humidity daily.
  - Spare so that we can have one down for maintenance and continue to operate.
    - That means dual power supplies in all devices, dual power distribution units, dual air conditioning units, and so on.
  - Our Network Command Center (NOC) provides 24 x 7 monitoring of entire compute and storage, physical, security systems.
    - The NOC also monitors every internet connection into all state offices.
    - In real-time monitoring of the Data Center's physical environment.
    - Most maintenance is performed during our off-hour maintenance window between 6 p.m. and 6 a.m.

DATA CENTER

EIS is driven by four core values:

Accountability

- We are responsible for quality outcomes and share information openly and honestly.

Customer centered

- We listen and seek to understand our customers’ needs.

Collaborative

- We build trust and establish mutual purpose to forge effective partnerships across the enterprise.

Innovation

- We simplify complexity, challenge conventional wisdom, and seek creative and useful solutions.

Q&A

- **What back-ups are kept for those agencies reliant on DAS?**

  Bend (Resiliency Site)

  - Mainframe – 100%, Standby
  - Midrange – 100%, Standby
  - X86 – 60%, Always On

- **What does DAS expect those agencies to be responsible for?**

  Restoration of systems and applications is the responsibility of the customer after DCS restores the infrastructure and platform.

Q&A (continued)

- **How does continuity work/look for those agencies reliant on DAS should there be a continuity event?**

  Backup Services provides data protection for files, virtual or physical servers. Backups are performed, stored, and maintained in multiple DCS locations. Managed backup and recovery is a fully managed solution that is configured, administered, monitored, and supported by the DCS team. Restores can be performed on-demand or via service requests by the customer.

- **What steps do those agencies need to take to prepare, prevent, and trigger a DAS IT continuity activation?**

  All agencies should have a disaster recovery plan for how they will recover after DCS restores the infrastructure and platform.

- **Is there assistance with exercises?**

  EIS/DCS customers fall exercise- last 2 weeks of October

Q&A (continued)

- **What are the Data Center Services:**
  - **Capabilities-**
    - 24/7 Command Center
  - **Resilience-**
    - Resiliency Site in Bend
  - **Response-**
    - Incident Management and Disaster Recovery Team
  - **Recovery resources**
    - Disaster Recovery Team
    - Annual exercise

Q&A (continued)

What are the Data Center Services:

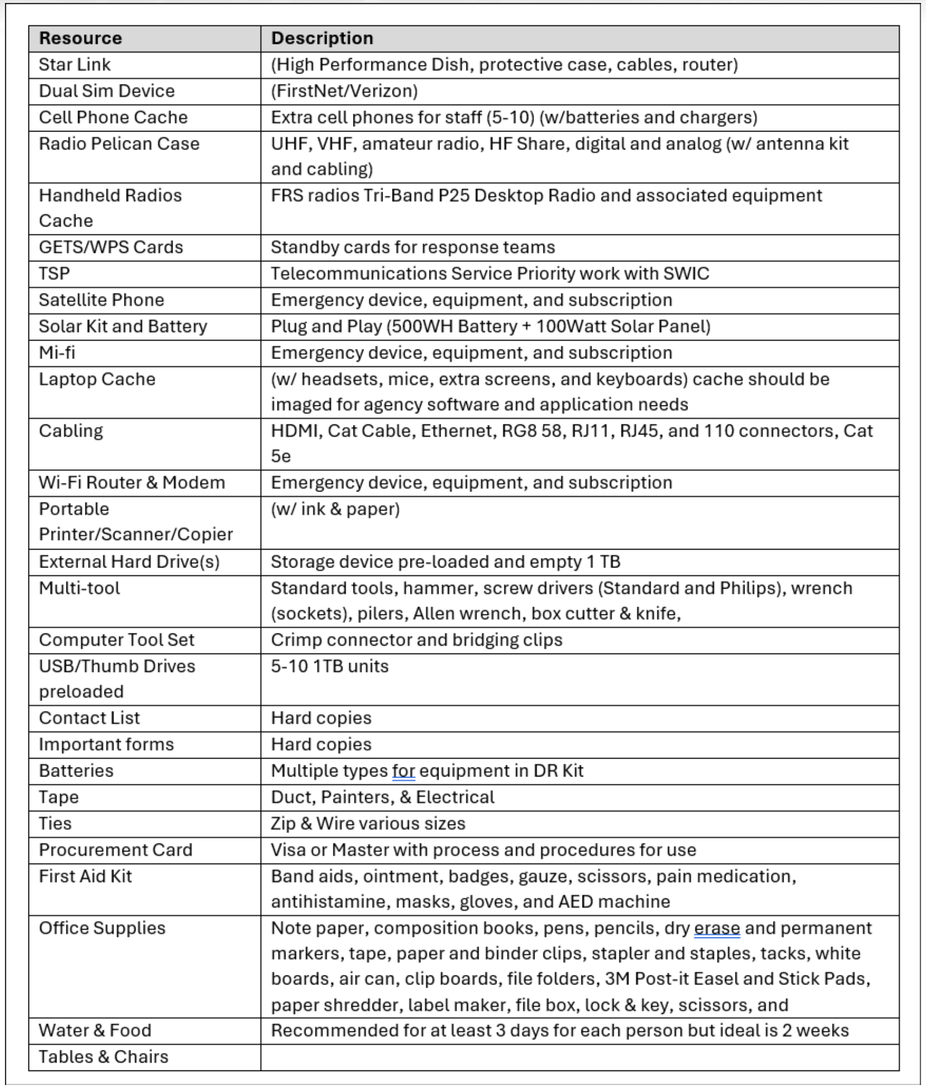
Supporting infrastructure

FUEL
DIESEL

- Smart grid agreement with PGE under the “dispatchable standby generation program” - PGE using our generators during peak electrical demand days (usually the hottest summer days) and covers the maintenance and provides the fuel for the generators. PGE tries to burn off about 1/3 every six months to keep fuel fresh. Outside and above ground diesel tanks hold a total of 10,000 gallons.
- 3 Caterpillar 1.5-Megawatt generators running, they'll burn about 90 gallons per hour. 1 generator provides 4 days of power for the floor at full capacity. Two are capable of fully supplying the Data Center with adequate power.
- 3 Cooling Towers. Chillers utilize “air side economizer” Use ambient air if 65 degrees or less. There are 3 chillers and run when needed.
- Our air-side economizers give us approximately 250-275 days a year of free cooling.
- Battery room – set to cover while generators kick on (20 second). Without generators, they would last about 45 minutes under full load. Under our current load, we have about 2 hours.
- Sprinkler system – Dry pipe, 2 event system: presence of smoke + heat required to set off; these are setup in zones to cover fire events.
- Water treatment – We use city water for everything, we purify the water that runs through the humidifiers.

Q&A (continued)

- **DR Kit example**



Resource	Description
Star Link	(High Performance Dish, protective case, cables, router)
Dual Sim Device	(FirstNet/Verizon)
Cell Phone Cache	Extra cell phones for staff (5-10) (w/batteries and chargers)
Radio Pelican Case	UHF, VHF, amateur radio, HF Share, digital and analog (w/ antenna kit and cabling)
Handheld Radios Cache	FRS radios Tri-Band P25 Desktop Radio and associated equipment
GETS/WPS Cards	Standby cards for response teams
TSP	Telecommunications Service Priority work with SWIC
Satellite Phone	Emergency device, equipment, and subscription
Solar Kit and Battery	Plug and Play (500WH Battery + 100Watt Solar Panel)
Mi-fi	Emergency device, equipment, and subscription
Laptop Cache	(w/ headsets, mice, extra screens, and keyboards) cache should be imaged for agency software and application needs
Cabling	HDMI, Cat Cable, Ethernet, RG8 58, RJ11, RJ45, and 110 connectors, Cat 5e
Wi-Fi Router & Modem	Emergency device, equipment, and subscription
Portable Printer/Scanner/Copier	(w/ ink & paper)
External Hard Drive(s)	Storage device pre-loaded and empty 1 TB
Multi-tool	Standard tools, hammer, screw drivers (Standard and Philips), wrench (sockets), pilers, Allen wrench, box cutter & knife,
Computer Tool Set	Crimp connector and bridging clips
USB/Thumb Drives preloaded	5-10 1TB units
Contact List	Hard copies
Important forms	Hard copies
Batteries	Multiple types for equipment in DR Kit
Tape	Duct, Painters, & Electrical
Ties	Zip & Wire various sizes
Procurement Card	Visa or Master with process and procedures for use
First Aid Kit	Band aids, ointment, badges, gauze, scissors, pain medication, antihistamine, masks, gloves, and AED machine
Office Supplies	Note paper, composition books, pens, pencils, dry erase and permanent markers, tape, paper and binder clips, stapler and staples, tacks, white boards, air can, clip boards, file folders, 3M Post-it Easel and Stick Pads, paper shredder, label maker, file box, lock & key, scissors, and
Water & Food	Recommended for at least 3 days for each person but ideal is 2 weeks
Tables & Chairs	

Best Practices

- **Develop the plan with a team of experts**
  - You’ll need the technicians and engineers
- **Identify critical software applications, hardware, and data required**
  - Look to your vital records as a good place to start
  - Conduct a Business Impact Analysis (BIA)
- **Evaluate and iterate the disaster recovery process**
  - What are your triggers for disaster recovery?
  - Do you have run or playbooks for your system/applications interruptions?
  - Who are your vendors? Do you know their plan? What are in their service level agreements?
- **Involve your employees and processes**
  - Train and educate your teams
  - Cross training
  - Exercise, Exercise, Exercise

Best Practices (continued)

- **Consider strategies such as backup and restore or cloud-based disaster recovery**
  - 3-2-1 approach

    3 – Keep 3 copies of any important file: 1 primary and 2 backups.

    2 – Keep the files on 2 different media types to protect against different types of hazards.

    1 – Store 1 copy offsite (e.g., outside your home or business facility).

- **Threat Assessment**
  - Check with your county for their Threat Hazard Identification Risk Assessment (THIRA) or use the states.
  - Conduct research on the FEMA National Risk Index Map | National Risk Index

Best Practices (continued)

- **Know your RTO and RPO**

  As part of the disaster recovery planning process, businesses also need to define its RTO and RPO as part of its recovery strategy:

  - Recovery Time Objective (RTO) - A business's RTO is how long it can tolerate an interruption to normal operations. This can be anything from a few minutes to many hours, depending on the nature of the business.
  - Recovery Point Objective (RPO) - The RPO refers to how much data the organization can stand to lose and is normally measured in time, such as an hour of data or 24 hours of data. A business that backs up once daily considers its RPO 24 hours.

Lessons Learned

- **Mutual Aid**
  - Who can you call for assistance:

    DCS

    www.itdrc.org

    MS365

- **Diagrams of Systems**
  - Flow chart of your infrastructure and applications
  - Input and output

- **Exercise your plan**
  - At least annually

Disaster Recovery Planning

- Assumptions and Situation
- System Descriptions
- Roles and Responsibilities
- Activation and Notifications
- Recovery Procedures
- Data Backup
- Inventory and Assets
- Vendor Contacts

EIS Website

- **Public Facing Website for EIS Customers- Resource**
  - Enterprise Information Services : Data Center Services : Data Center Services : State of Oregon
    - https://www.oregon.gov/eis/data-center-services/Documents/eis-dcs-service-catalog.pdf
    - https://www.oregon.gov/eis/data-center-services/Documents/eis-ss-enterprise-technology-services-service-level-agreement-v1.2-signed.pdf

ENTERPRISE
information services

Kathleen Silva

Business Continuity Manager

Enterprise Information Services

Data Center Services

Cell: (971) 701-5422

kathleen.silva@das.oregon.gov>