**Oregon State University**

**Information Technology**

***Business Continuity – Disaster Recovery Plan***

***For OSU’s Enterprise Resource Planning (ERP) Systems***

**Redacted**

**August 2024**

**Prepared by Kent Kuo, Director, IT**

Last Revised: Redacted Version XIII, August 2024

**Table of Contents**

# Business Continuity-Disaster Recovery Approval & Revisions

Management Acknowledgement & Approval [4](#MAA)

Record of Revisions [5](#REVISIONS)

# The Plan

Introduction [6](#INTRO)

Objectives and Purpose [7](#OBJ)

Scope [7](#SCOPE)

Maintenance and Approval [8](#MAINT)

Testing [8](#TEST)

Training [9](#TRAIN)

Activation [9](#ACTIVATION)

**Tiers of Disruption (TOD) & Prevention**

Tier 1 [11](#TIER1)

Hardware Resiliency [11](#HW)

Software Resiliency [12](#SW)

Data Resiliency [13](#DATA)

Cyber-Attack Resiliency [13](#CYBER)

Tier 2 [14](#TIER2)

Network Fiber Resiliency [15](#NW)

Building Resiliency………………………………………………. [15](#BLDG)

Catastrophic Event [16](#CATESTROPHIC)

Cloud Native Strategy [16](#CFS)

**Crisis Response Procedures**

Notification [18](#NOTE)

Alternate Communications [18](#ALTCOMM)

Incident Command Post (ICP) [19](#ICP)

Mobilization [19](#MOBILIZATION)

Disaster Recovery as a Service Activation [19](#RESTART)

Post-Mortem Review and Incident Report [20](#PMORTEM)

**Business Continuity – Department Engagement**

Business Continuity Processes [21](#BCPROCESS)

**Addendums**

Addendum A (Network Topology) [22](#ADA)

Addendum B (ERP Hardware Infrastructure & Database Software Architecture) [23](#ADB)

Addendum C (IT-IMT Communications Response) [24](#ADC)

Addendum D (Data Center and Communications Redundancy Overview) [30](#ADD)

Addendum E (IT Emergency Contact Information) [31](#ADE)

Addendum F (Test/Maintenance Log) [33](#ADF)

Addendum G (Vendor Cloud Backups) [34](#ADG)

**Business Continuity-Disaster Recovery Approval & Revisions**

**Management Acknowledgement & Approval**

The Business Continuity-Disaster Recovery Plan for Oregon State University’s Enterprise Resource Planning (ERP) systems was prepared to maintain a viable response capability and to establish a comprehensive approach to emergency management across three significant Tiers of Disruption (also known as TOD). This plan applies to all IT personnel participating in the mitigation, preparedness, response, and recovery efforts. Under the University’s Chief Information Officer (CIO), the Executive Director shall be responsible for plan oversight and coordination with applicable stakeholders. The BC-DR plan is based on the TOD concept, which plans for natural and man-made disasters and incidents while following the National Incident Management System (NIMS) guidance. The plan is flexible in that either specific parts or the entire plan may be activated, based on the emergency and decisions by University senior leadership. Additionally, this plan is a sub-component of the University’s larger Emergency Operations Plan (EOP) and is designed to fit within that framework. This BC-DR Plan supersedes and rescinds all previous editions. The BC-DR Plan and its supporting contents are hereby approved, and the plan is effective immediately upon the signature of the authorities listed below.

**Approved:**

Name, Title, Organization Date

**Record of Revisions**

|  |  |
| --- | --- |
| **Date** | **Changes** |
| Redacted | Redacted |
| Redacted | Redacted |
| Redacted | Redacted |
| Redacted | Redacted |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**The Plan**

**Introduction**

Beginning with the implementation of Software in 1990, the University has increasingly utilized technology to drive its business operations. This past year, leveraging technology has proven to be one distinctive factor in the institutions ability to operate and thrive. The dependence on IT resources has been shifting from hardware and software directly supporting individual applications to a “local cloud” model where hardware is configured to support multiple applications. Additionally, since 2021, OSU has adopted a “Cloud Native” strategy where we work with vendors to run any needed applications in a vendor cloud which has multiple data centers in different geographical regions for business continuity and disaster recovery purposes. As such numerous business applications have been shifted to or originally established in the “cloud”. Consequently, these applications (see [Cloud Native Strategy](#CFS)) have a built-in business continuity and disaster recovery plan (BC-DR) defined by the contract between the University and the application vendor and are not part of this BC-DR plan.

That said, it has also become true that the “network is the computer” in that the University now has a heavy reliance on the University’s optical network. That reliance was eminently clear during the 2020 COVID-19 pandemic when most of OSU’s staff and students had to work, teach, and learn/study remotely. Also, in 2010 OSU experienced a tunnel fire which melted part of the University’s optical network. Since that time, the University has invested in dual path network on OSU’s main campus, established a second head-end for data going to and from the main campus, and has entered a multi-institution/state acquisition of optical fiber across the state of Oregon to ensure access to multiple nodes of the Internet 2 infrastructure.

On November 28, 2021, OSU completed the shift of its administrative systems portfolio into Vendor’s Infrastructure as a Service (IaaS) Cloud. This migration encompassed almost all aspects of OSU’s business applications supporting multiple campuses. The Administrative Software set of applications encompassing Finance, Financial Aid, Human Resources/Payroll, Student Information Systems, and the Vendor Operation Data Store (ODS), along with other essential business applications now reside within Vendor’s Cloud Infrastructure (Cloud) which has been established across three Vendor data centers within the City, State region. Additionally, all backups of the data/databases, applications, operating systems, and other file systems are backed up to Vendor’s Cloud backup service. Finally, OSU has also undertaken to build a secondary Disaster Recovery site for the production systems homed in the City, State region, in Vendor’s City, State region.

When considering what to include in a business continuity plan, one needs to address the risk of something happening in terms of probability of happening and impact if it does happen. Consider for a moment the impact of a disaster which prevents the use of the system to process Student Registration, Payroll, Accounting, or any other vital application for weeks. Students and faculty rely upon systems for instruction and research purposes, all of which are critically important to the core business of the University. It is hard to estimate the damage to the University that such an event might cause. A fire, earthquake, or other regional impactful event could easily cause enough damage to disrupt these and other vital functions of the University within Vendor’s City, State facilities. Without adequate planning and preparation to deal with such an event, the University's enterprise applications could be unavailable for many weeks which would prevent the academic mission of the institution to operate.

The University has grown to expect a high level of service availability. A disruption of these services would become a major obstacle to the day to day administration and delivery of educational services. It is the essential nature and high level of organizational dependency on these services that has prompted IT to update its BC-DR Plan.

**Objectives and Purpose**

The objective of this BC-DR Plan is to address two tiers of potential business disruption (also known as TOD) with respect to its enterprise application systems. The activation of any response to a TOD is dependent on the exact circumstances of the disruption. However, activation will automatically kick in if the VP-UIT/CIO decides to do so during or immediately after the initial 72-hour window begins from the onset of the outage. A **Tier 1** disruption focuses on the loss of hardware, software, data corruption, and/or cyber attack associated with an application. A **Tier 2** disruption focuses on the partial or complete loss of the production Cloud infrastructure in City, State supporting the administrative systems portfolio or part of the campus’ optical network.

This BC-DR plan will identify the manner in which OSU has planned for the restoration of critical and essential ERP services within each Tier of disruption to the campus community within as short a time period as possible. In the event of an extended outage, this plan describes the collaboration which will allow core operations departments to plan for how they will function without the ERP system beyond the initial 72-hour outage window.

Primary objectives of the Plan include:

* Describe each Tier of Disruption and the preventative measures and/or mitigating controls being taken to address the various possibilities of an unplanned outage.
* Document which key business operations are within a vendor cloud and which would **not** be impacted by a Tier 1 or 2 disruption within the production environment in Cloud.
* Assess preventive actions, incident management processes, and identify an organization structure to support restoration of services for each Tier of Disruption.
* Delineate procedures that facilitate decision making to restore critical services within each TOD.
* Document and maintain changes to the specific resources needed to implement the necessary restoration of services at each TOD.
* Provide personnel information, along with supporting policies and procedures to support the recovery process.

**Scope**

Oregon State University has an Emergency Operation Plan (<https://emergency.oregonstate.edu/sites/emergency.oregonstate.edu/files/2022_osu_emergency_operation_plan-signed.pdf>), which addresses the campus-wide need for disaster management readiness and a structure to cope with service disruptions or hazards/disasters. The IT’ BC-DR Plan will address the more specific ERP vulnerability of the software and hardware resource (aka ERP IT Systems and Data Failure) aspects of the larger Emergency Operations Plan. The scope of the BC-DR plan will be limited to the Information Technology (IT) Enterprise Architecture, IT, and Network Services staff, hardware, and software as it relates to the production site in Vendor’s City, State region.

**Maintenance and Approval**

The initial BC-DR plan will provide a resource and a road map to cope with service outages at each TOD. Unfortunately, plans quickly become outdated as the organization’s structure, personnel, equipment, and services change. For these reasons, a maintenance program must be adhered to which will keep the BC-DR plan current and maintain its value on an ongoing basis. Maintenance procedures for the Plan are as follows:

* A major organizational change within ITwill prompt the IT VP/CIO (and/or Executive Director for TSA) to request the Director, IT to initiate a review and/or update of the BC-DR plan.
* Equipment replacement or updates which may impact the plan, along with major changes in services provided or services received, will be reviewed annually during the month of March by the Director, IT, and also require a review and/or update to the BC-DR plan.
* Any shift of an application into a vendor cloud external to the University will be recorded annually during the month of March by the Director, IT and also require a review and/or update to the BC-DR plan.
* Any determination of exposure from a cyber-attack will be reviewed annually during the month of March, and also require a review and/or update to the BC-DR plan by the Chief Information Security Officer.
* Annually, during the Summer quarter, the BC-DR plan will be organized by the Director, IT and include a table top exercise and/or DR failover test to ensure all engaged staff are appropriately informed about processes, roles, assignments, priorities, and escalations associated with the BC-DR plan.

After restoring a service failure, the BC-DR plan should be reviewed to see if information can be included in the BC-DR plan to facilitate a smoother, faster recovery, should a similar incident occur in the future.

Changes to the BC-DR plan are recorded in the Test/Maintenance Log, also included in [Addendum F](#ADF).

**Testing**

Full failover testing of the BC-DR plan can be accomplished in several ways within Vendor’s Cloud Infrastructure. Consequently, it is reasonable to periodically engage in failover processes and procedures to assure the completeness and adequacy of the documentation and recovery procedures described in the BC-DR plan without significant disruption to essential business operations. Therefore, the following testing guidelines will be followed:

* Annually, OSU will utilize both its production and non-production environment to test the main elements of a failover procedures and to ensure documentation is accurate and current.

The results of all test activities will be documented and used to update and improve documentation and procedures included in the BC-DR plan. Testing and improvement activities should be noted in the Test/Maintenance Log that is provided in Addendum F.

**Training**

As new staff are added and existing staff either change roles and/or leave the University, it is imperative that an annual training event be held to acclimitize IT– Enterprise Architecture, IT, and Network Services staff to the existence, details, roles, and processes associated with business continutity and disaster recovery. Utilizing the annual test of the BC-DR plan, OSU will work with its Disaster Recovery as a Service (DRaaS) contractor to walk through each element of a failover to help cement clarity around what will happen and which responsibilities are delegated to whom in varying levels of a TOD. As such, the Director of IT will minimally hold an annual BC-DR test for new staff and existing staff of the process and roles, in August of each year. It is also recommended that this failover training happen at least twice (in addition to the annual official failover test) to ensure all systems and staff are syncronized and trained on their respective responsibilities if a real failover was required.

**Activation**

This BC-DR activation plan factors in both Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO refers to the institution’s tolerance for data loss, or the amount of data lost before significant harm is done to the institution. RTO refers to how much time an application can be down without causing significant damage to the institution. Applications are often defined by the institution’s business processes risks/risk tolerance, requirements, and criticality, and correspondingly can have different tolerances for down time.

With the shift to Cloud, all of OSU’s enterprise business systems, tools, backups, and infrastructure are in Vendor’s Cloud and we have worked with OSU’s Disaster Recovery as a Service (DRaaS) service provider (Vendor) to establish a new Disaster Recovery site in Vendor’s City, State facility. Utilizing this new DRaaS option, OSU’s RTO would be two hours and the RPO would see 15 minutes of potential loss of data with a failover to the alternate City, State facility. If the restoration requires going to online backups, the RPO would be an hour of potential data loss.

With both RPO and RTO in mind, OSU’s BC-DR plan can be activated through two primary methods:

* A Tier 1 or 2 disruption which impacts the ERP operating environment will activate the BC-DR plan. This type of activation may be initiated by the Chief Information Officer, the Executive Director, the Director of IT, or a member of the CIO Executive Leadership who has been made aware of the emergency. Emergency members of the IMT may also become involved and are identified in the Emergency Contact Information list included in [Addendum E](#ADE).
* In the event of a major disaster or emergency on OSU’s main Corvallis campus, the Oregon State University, Emergency Operation Plan (EOP), will be activated which will subsequently require implementation of departmental plans. A major disaster in Corvallis would not impact the availability of OSU’s systems in City, State. It may, however, impact the ability of people in Corvallis to access systems within Cloud. This type of activation will be declared by a senior University administrator with directives passed through the emergency chain of command, most likely through the Incident Management Team (IMT) or Emergency Operation Center (EOC) as identified in the OSU EOP at:

<https://emergency.oregonstate.edu/sites/emergency.oregonstate.edu/files/2022_osu_emergency_operation_plan-signed.pdf>.

Any activation of the BC-DR plan will initiate the assembly of the IMT as described in the [Crisis Response Process](#CRISIS) section of this document.

**Tiers of Disruption (TOD) and Prevention**

**TIER 1**

The first level of potential loss is defined by a Tier 1 level of disruption. A Tier 1 disruption focuses on the loss of hardware, software, data corruption, and/or cyber-attack associated with an application. To mitigate impacts of a Tier 1 disruption, we have built in hardware, software, and data resiliency with the objective of maintaining redundant systems and defined recovery practices. This built-in resiliency will allow us to restore systems and recover from potential loss of data, impact on an application from hardware failures, and/or a potentially crippling event such as a cyber-attack.

**Hardware Resiliency**

The loss of hardware can happen at the network, firewall, load balancer, application server, database server, and storage layers. To account for any potential loss of equipment within Cloud, IT has established a robust solution to account for these potential points of failure:

**Network (see** [**Addendum A**](#ADA)**):**

**Firewall:** OSU has established six cloud based Firewalls within Cloud. Two are for OSU’s production site, two for a testing site, and two for the DR site. Having two allows OSU to failover from one firewall to the other if there is some problem with the initial firewall in use. Each firewall is sized to be able to handle the network traffic going to the load balancers in front of the ERP applications.

**Routers/Switches:** On the OSU campus, OSU has multiple/redundant network routers, on-premises firewalls, VPNs, and switches for network resiliency.

**Load balancer:** The application servers are behind two separate and redundant load balancers in two separate availability zones for network traffic resiliency.

**Server and Storage Infrastructure (see** [**Addendum B**](#ADB)**):**

**Application, middleware, and job servers:** OSU has allocated 70 virtual machines (VMs) to support the application, middleware, and job server aspects of its ERP infrastructure. In Cloud OSU utilizes Vendor’s Console to monitor the health of its guest VMs. In the event any individual VM fails, Vendor will automatically initiate a new VM. Under this model, OSU has established resiliency with respect to the application layer of the ERP infrastructure.

**Database servers:** OSU has established 14 individual database servers using Vendor’s Database as a Service (DBaaS) feature within Cloud for its ERP infrastructure. The DBaaS feature enables Vendor to monitor the health of an Vendor DB. If it discovers the hardware underneath a DB has issues, it will notify OSU DBA staff and allow them to schedule a reboot. If that doesn’t happen by a deadline date established by Vendor, Vendor will do that for OSU. If a DBaaS server fails unexpectedly, Vendor’s DBaaS will reboot the entire DB on a different server and restart the DB from that server.

**Storage/SAN:** OSU utilizes the Vendor Cloud Infrastructure File Storage. This Cloud storage solution from Vendor employs 5-way replicated storage across different server racks, located in different fault domains, to provide redundancy for resilient data protection. Data is protected with erasure encoding.

The File Storage service uses the "eventual overwrite" method of data eradication. Files are created in the file system with a unique encryption key. When you delete a single file, its associated encryption key is eradicated, making the file inaccessible. When you delete an entire file system, the file system is marked as inaccessible. The service systematically traverses deleted files and file systems, frees all the used space, and eradicates all residual files.

**Online Backups:** OSU takes advantage of Vendor’s Cloud (Cloud) Backup service for all the database, operating system, and software file system backups (see [Addendum G](#ADG) for details).

**System Health Monitoring:** IT utilizes a series of system checks and notifications in the event an unplanned outage occurs. Staff uses several solutions to monitor the health of the ERP systems. Within Cloud, Vendor Console to monitor all VMs and Vendor Enterprise Manager monitors all the DBaaS servers. Cron jobs and Vendor scheduler are used to check on specific accounts/connections to see if they are either hung or locked. Logs are scanned for errors in Self Service, staging tables, or Apache file logs. Finally, checks are made to ensure SFTP, JVM memory, log on attempts to a production database are working, and whether database schemas are running over their disk space quotas, are integral to the continuous health checks being made to the ERP systems.

**Software Resiliency**

**OS, Database, and Software file systems:** The file systems for the Vendor Linux operating systems (OS), the Vendor Relational Database Management System (RDBMS) executables, and application files for Administrative Software are backed up to Vendor’s Cloud Backup service.

**Identity and Access Management Infrastructure:** The Oregon State University Information and Technology, Identity and Access Management infrastructure uses a combination of redundant systems and backups. These core systems include LDAP and login systems. OSU Login uses LDAP and has two systems that are redundant at our campus location and well as geographic co-location where two systems reside in Amazon Web Services (AWS).

We use split-DNS for ONID LDAP and OSU Login. Off-campus DNS queries use AWS's Route # service which performs health checks on the AWS-hosted and on-campus nodes of ONID LDAP and OSU Login. Route # will return DNS responses that map to AWS-hosted services or, if the AWS-hosted services are unavailable, the on-campus Netscaler load-balancer. On-campus DNS queries return the Netscaler load-balancer.

For backups, OSU IT uses virtual machine backups managed by internally by OSU IT Technology Infrastructure Services. Backups are done using a software tool called Software. Daily snapshots are taken of the critical virtual machines. Other ancillary systems would have to be restored but are not critical for every-day functionality.

**Change Management:** IT adheres to and maintains its change management policy and processes for most of the systems under its purview (https://oregonstateuniversity.sharepoint.com/sites/UIT/SitePages/IT-Change-Management.aspx). Relative to OSU’s ERP systems, upgrades are standard changes in the Change Management process. Each upgrade, however, has corresponding documentation that is reviewed by both technical and appropriate business owners and plans for backout/communications. The upgrade is first installed into the development environment. If there is an impact to any locally modified object, those objects are put into the queue to reapply the modifications to the new upgraded object from Vendor. Those newly modified objects are then tested by the appropriate business owner in a “Pre-PROD” environment that mirrors the actual production environment, before being signed off on and moved into production. Tickets are closed after the change is run in production for two weeks to ensure no issues arise. Departments have established individuals responsible for submitting any changes for that department. Each department rates the priority of their changes to ensure more critical changes are worked on before lower priority changes. Significant changes include communication plans and back-out plans.

**Data Resiliency:**

**Vendor Archive Logs:** OSU utilizes Vendor’s archive logs to manage individual transaction processing. This requires OSU to backup to tape ~3TB of archive logs every 24 hours. This is done by using Vendor’s Cloud Backup service and automatically backing up the archive logs every hour. This allows OSU to be able to restore the data in the Vendor database to a specific point-in-time or to the “current” point-in-time. This ensures the institution can restore its data as it needs to in the event of a cyber-attack and/or loss of hardware or software. Additionally, backup reports are generated which check for the archive logs remaining after the archive log backup completes.

**Tape Backups:** OSU takes advantage of Vendor’s Cloud (Cloud) Backup service for all the database, operating system, and software file system backups (see [Addendum G](#ADG) for details).

**Incident Management:** IT updated its incident management policy (<https://is.oregonstate.edu/sites/is.oregonstate.edu/files/projects/incident-response-policy.pdf>, 2013), and established an Incident Management Team and process (see Addendum C, 2016). All major unplanned outages of the ERP suite adhere to the incident management policy and the IMT process in managing these unexpected outage incidents. This includes an incident post-mortem review and report of the incident, the root cause, expected changes to ensure such an event does not occur again for the same reason, and a timeline for changes if needed.

**Cyber-Attack Resiliency:**

**Account/Password Hacking:**

**Single Sign On:** access is single sign-on. All new employees are set up with a unique employee ID as well as a unique user ID which is required to obtain access to the approved applications via password authentication. Password management is managed using Vendor Enterprise Directory Plus Lightweight Directory Access Protocol (LDAP) solution. All passwords are established to comply with the NIST 800-63 recommendations on passwords. This includes maintaining a password history to avoid repeating passwords that have previously been used; an account lock after 10 unsuccessful attempts; and a 30-minute time delay on the lockout period after an account has been locked. Additionally, the use of Multifactor Authentication (see below) further enhances accounts from being hacked.

**Phishing:**

**Multifactor Authentication:** OSU Login, also known as OSU Single Sign-On (SSO) allows users to access multiple OSU applications with one login. It consists of four nodes: two on premises (on OSU campus) and two in the cloud (on AWS). OSU Login depends on other infrastructure components, such as power, network, and DNS. The Identity and Access Management (IAM) team will collaborate with OSU IT staff in case of any disaster recovery situations that require configuration changes.

**Ransomware Attack:**

**Backups and Archive Logging:** OSU has established a Disaster Recovery as a Service (DRaaS) with Vendor in the event there is a ransomware attack which impacts the ERP server infrastructure within Cloud. OSU would be able to restore its systems, application software, databases and data to a previous (non-impacted) image of its middle tier application services and to its hot stand-by databases within the DRaaS site. The expected RTO is two hours and the RPO would be 15 minutes of data loss from the failover. OSU also backs up data changes for the system within Vendor archive logs which are backed every hour. Thus, if/when a ransomware encryption is triggered, Vendor/ will immediately shut down. All data between the production site (City, State) and the DR site (City, State) would stop propagating once a ransomware attack encrypts even a single database file. This model allows OSU two options for recovery. The first is to start up the DRaaS hot stand-by databases. In this use case OSU may see as much as 15 minutes of data loss. The second is to rebuild the databases (if desired) from the Vendor Cloud backups. In the latter case it is possible that OSU could experience as much as an hour of data loss.

­

**Random Hacking Attempts:**

**Database Encrypted at Rest:** The Vendor Cloud Infrastructure service includes the encryption of the database at rest. This helps to ensure hackers cannot copy the database and mine its contents.

**Data Encrypted in Transit:** All data going into and out from the Vendor Cloud is encrypted in transit.

**Hardened Images and Microsoft Defender:** OSU has deployed CIS benchmark compliant hardened images for all the application servers within Cloud. Microsoft Defender Endpoint (malware) has also been installed on the middle tier application servers within Cloud.

**Network Security Monitor and Intrusion Detection:** OSU rearchitected its server certificates to reside on the Firewalls. This allows the traffic behind the firewalls to operate in plain text. This further allowed OSU to forward database logs to OIS’s Azure destination for intrusion detection. Additionally, OSU IT staff installed the Advanced Intrusion Detection Environment tool (AIDE) on all its middle-tier application servers to scan for changes in root devices and email changes).

**Vulnerability Scanning:** Cloud also has a vulnerability scanning service that OSU utilizes for vulnerabilities. At the DB level, OSU utilizes Vendor’s DBaaS, which allows OSU to be sure the databases are on managed database servers where configuration options are limited, and security updates are monitored and applied by Vendor. Additionally, OSU has public facing IP space scanned continuously by CISA, with a weekly summary report provided. Finally, OSU has deployed Firewall’s IP reputation filtering service.

**TIER 2:**

The second level of potential loss is defined by a Tier 2 level of disruption. A Tier 2 disruption focuses on the partial or complete loss of the production Vendor Cloud region in City, State or part of the campus’ optical network. OSU’s use of Vendor Cloud is built across three separate data centers in the City, State region. Vendor has an alternate site in City, State.

The greatest potential threat to Vendor’s Cloud region in City, State would be characterized as a large-scale regional outage caused by some natural (or possibly man-made) disaster. Such a disaster (massive wildfire, flood, tornados, 9.0 level earthquake, temporary power surges/blips, extended loss of power, loss of connectivity, etc.) would have to have compromised the entire City, State region or the electrical grid/network infrastructure within the City, State region. This section identifies some of the risks that exist and preventative actions that have been taken.

**Corvallis Campus Network Fiber Resiliency:**

**Fiber Backbone:** Campus networks are defined by optical fiber cabling across campus. Two major fiber runs (see map below - REDACTED) ensures that the Data Center (Availability Zone #1) has fiber going to the two major network head-ends for the Corvallis campus. The first head-end is in the First Building (Availability Zone #2). The second head-end is in the Second Building: Availability Zone #3). Single-mode fiber or high-capacity fiber has redundant paths established between all three availability zones (see Addendum D).

**Building Resiliency:**

**Head-End Redundancy:** In 2015, OSU determined that it needed a more robust redundancy for both the network head-end into the Corvallis campus and a backup machine room in the event the First Building (where the first network head-end terminates) was determined to be operationally unsound or uninhabitable. As such, the Second Building was built in 2016 and made operational in 2017. It was also built far enough away from the First Building network head-end so that an event that could be impactful to those two sites may not pose the same risk to the Second Building and any IT services established in the Second Building.

**Catastrophic Event (i.e., 9.0 Earthquake, Wildfires, Tornados, Explosions):**

9.0 Seismic Earthquake: While the threat of an earthquake in the Corvallis area is low (it is 50% more likely that a significant earthquake would be off the coast of Oregon or in the Portland region), it should not be ignored. Scientists have found through recent study that Oregon has an earthquake recurrence interval of approximately 300-600 years. The last event occurred around 300 years ago. Therefore, there is a strong possibility of a subduction zone earthquake of a magnitude greater than 8 within the next 300 years. Additionally, climate change has illustrated the dangers associated with widespread wildfires and tornados. Finally, a man-made event (explosions) cannot be ruled out either. IT, consequently, has approached this level of disruption in two significant ways: Vendor Cloud with Alternate Disaster Recovery as a Service Site for all and corollary administrative applications; and Cloud Native for other secondary and tertiary application systems.

**Vendor Cloud:** In November 2021, OSU moved its entire application suite (HRIS, FIS, SIS, and Financial Aid) and corollary applications into Vendor’s Cloud in Vendor’s City, State region. Additionally, OSU entered a contract with Vendor to provide a Disaster Recovery as a Service (DRaaS) solution for an alternative DR Site within Vendor’s Cloud Infrastructure in their City, State region. The alternative DR site has duplicative firewalls, load balancers, middle-tier application servers (warm configuration), and Vendor databases (hot configuration). This environment is designed to allow OSU to be able to failover within two hours with an expected data loss of 15 minutes. When the University decides it can fail back, it can do so at a date/time it determines within no expected data loss.

**Cloud Native Strategy:** Since 2021, IT has been working with OSU’s administration to adopt a “Cloud Native” strategy with all new implementations of software functionality at OSU. Cloud Native recognizes the value of the deployment of new vendor capabilities in either a public cloud or a vendor-specific cloud. In doing so, these application vendors must demonstrate how they are resilient from regional level disasters/disruptions through the existence of a BC-DR strategy where data centers exist in different geographical zones within the U.S. They must also meet stringent security requirements reviewed and approved by IT Staff as part of an acquisition process and before contracts are signed. These requirements include data encryption in transit and at rest, single sign-on, and multifactor authentication support as defined by OSU. Consequently, numerous business functions have been moved to the “cloud”. These include:

**Employees:**

Employee Applications

Employee Training

Student Employee Applications

Time & Attendance Tracking

**Finance:**

Campus Event Calendaring

Electronic Procurement and Contract Management

ID Card System

ID Card System – Cascades Campus

Student Accounts Receivables

**Misc:**

Electronic Signature System

Emergency Notification System

Enterprise Document Management

Institutional Drupal Web Hosting

Medical Electronic Records Backups

Telecom Management

IT Service Management Ticketing System

**Research:**

Research Compliance Systems

Research Pre-Award Management

**Student:**

Automated Room Scheduler

Campus Housing Applications

Career Services

Curriculum Management

Electronic Student Evaluation of Teaching

Faculty Vita

Graduate Admissions

New Student Orientation

Online Catalog of Courses

Online Schedule of Classes

Scholarship Management

Student Athletics Ticketing

Student Class Scheduling

Student Conduct

Student Learning Management

Student Math Placement

Student Mobile Applications

Student Sexual Assault and Alcohol Safety Training

Study Abroad

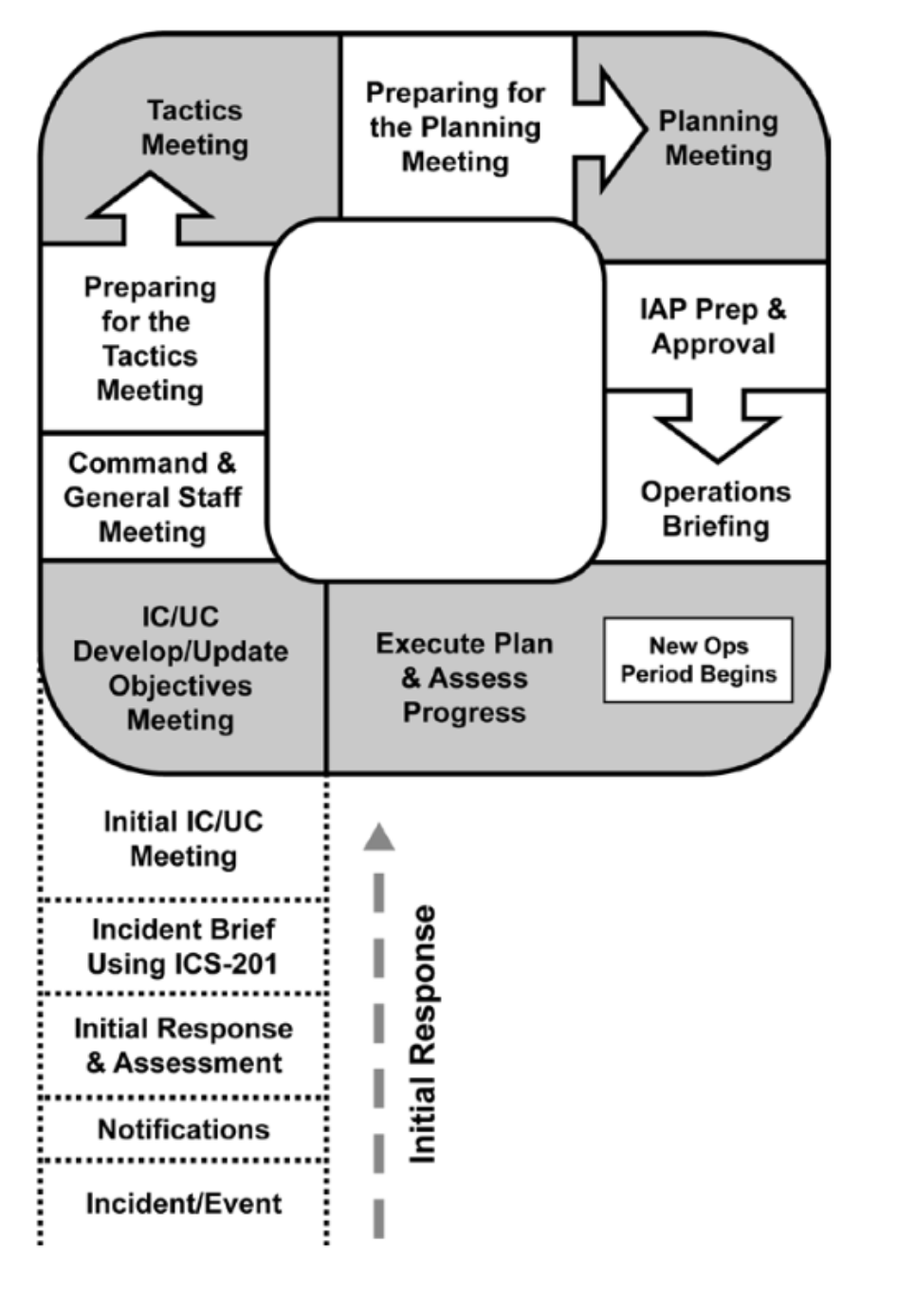
Transcript Request Processing

Undergraduate Recruiting and Applications

**Crisis Response Procedures**

**Notification**

If a disaster is declared by the administration of Oregon State University or if a major loss of service is experienced by IT, the IT Incident Management Team (IMT) should be called together in line with the Planning “P” model adopted by both OSU’s Emergency Operations Planning team and United States’ Federal Emergency Management Agency (FEMA).

****

IMT’s Process (see [Addendum C](#ADC)), reflects OSU’s IMT model where unplanned outages are initially managed by the unit and can be scaled to be coordinated at an institutional level if such an escalation is deemed necessary (see Incident Command Post below). An unplanned outage of the ERP system defaults the Incident Commander (IC) role to the current Director, IT. Any number of other ITdirectors and executive directors may also pick up the IC role in the event the default individual is not available. The Operations Chief role is often filled by the various Associate Directors within IT, and the Communications Lead can also be anyone listed as a resource on the IMT team.

An incident is often assessed by the IC as to whether the unplanned outage is short-term in nature (i.e., less than 30 minutes), or if the investigation into the cause and restoration of services will take longer than an hour. In that initial assessment by the IC, OSU has determined that the IC will notify the rest of the IMT using the Emergency Notification System (aka OSU Alert), that they have assumed the IC role, and asks for another IMT member to take on the communications lead role. If a determination is made that this outage will take longer than two hours to assess and/or resolve, the IC/Communications Lead will organize a meeting with key stakeholders every two hours to discuss what is known, what is being done, ask about impact, and discuss what steps various core offices can do to maintain business operations until the system is returned to service. In this way clear communications about the unplanned outage, activities being taken, and plans for business continuity can occur.

**Alternate Communications**

In the event of a major catastrophic event, the OSU Emergency Operations Plan (EOP: <https://emergency.oregonstate.edu/sites/emergency.oregonstate.edu/files/2022_osu_emergency_operation_plan-signed.pdf>) will be followed. The EOP has a designated Situation Assessment Team (SAT) which will decide if/when to recommend the activation of OSU’s Incident Management Team (OSU-IMT).

As needed the OSU-IMT will further activate the Crisis Communications Plan (<https://oregonstate.app.box.com/s/vxgwi4o68l91wsg8g8bqy2r83lvq7dms>), which also uses the Emergency Notification System (aka OSU Alert), to assist in providing alternative communications services as needed. OSU Alert is a cloud-based system which can send out communications in the form of text, email, and phone messages to all students, faculty, and staff within 15 minutes (and often far less). Cell phones will be the first alternative for disrupted campus communications services. The EOP will coordinate with both the call center and radio communications as needed.

In some instances, local disruptions to telephone services may best be worked around by dispatching foot messengers for campus communications.

**Incident Command Post (ICP)**

IT and OSU both utilize FEMA’s Incident Command System (ICS) model. An ICP can be established for each area autonomously, until the problem is deemed to be widespread and requiring the institution activate its EOP and ICP. Correspondingly, as per the IMT process, if the unplanned outage is determined to continue over an extended period, an Incident Command Post (ICP) will be designated and all IMT members will be informed of the location of the ICP. If the problem continues to escalate OSU can choose to activate an institutional ICP to coordinate activities.

**Mobilization**

The first task for the Incident Commander (IC) is to gather the requisite technical staff and initiate an assessment of the unplanned outage. Technical staff will then provide an assessment as to whether the unplanned outage is significant in both nature and in the effort to return the application to service. If in this assessment the IC believes this to be an event that will exceed one hour, the IC will use OSU Alert to notify the IMT that IC has been assumed and request another member of the IMT take on Communications Lead.

This assessment should include the nature of the problem, scope of the problem, impact on services, resources required to resolve or mitigate the problem, and notification of parties effected. The next step will be to prioritize emergency actions and responses, followed by communication of critical information and instructions. The assessment of the incident will dictate what resources need to be available to bring about a solution. These resources may include regular or additional staff, vendors, users, and contractors, along with hardware or components and auxiliary equipment such as pumps or generators. User Reaction Plans will provide information on critical process and user alternate service options.

# Disaster Recovery as a Service Activation

There are four named roles who can activate a Disaster Recovery failover from the City, State region to the City, State region. These four roles are: OSU’s Chief Information Officer, OSU’s Deputy Chief Information Officer, IT’s Executive Director, and the Director, IT. Any of these four roles are designated contact points for Vendor Business Solutions and can request the activation of the DR site in City, State. OSU and Vendor have already built the DR site and have drafted up a “Run book” which details the exact process for activating all the essential applications OSU requires to manage its daily central operations.

**Post-Mortem Review and Incident Report:**

After any crisis has been resolved, the designated IC for the unplanned outage hold a post-mortem review to better understand root cause of the unplanned outage, what took place during the outage, and what lessons were learned to better ensure any potential mistakes are not repeated. Additionally, the IC will provide a thorough Incident Report documenting time, date, root cause, activities that occurred during the outage, communications efforts, and what steps are being taken to mitigate the potential for a repeat of that outage. This report will be submitted to and reviewed by the IMT to ensure it is complete and/or request for greater clarification or follow through as events warrant. This is also an opportunity for the IC to identify changes in content and procedures that will make the BC-DR Plan more useful, should a similar incident occur in the future. Updates or notes for updates to the BC-DR Plan should be made as soon as practical both to capture fresh incident information and to have a current Plan available for future access. All changes to the Plan should be noted in the Maintenance Log in [Addendum F](#ADF).

**Business Continuity – Department Engagement**

**Business Continuity Processes:**

After an unplanned outage occurs, the IMT process includes a recurring every two-hour communications update for key stakeholders associated with the core operations of the ERP system. This recurring meeting with key stakeholders will be organized by the IMT-Communications Lead to happen every two hours over the duration of the outage. The purpose of these recurring meetings is to ensure all stakeholders understand the current understanding of the root cause of the outage, the steps being taken to resolve the outage, and the anticipated timeline of events to fully restore operations. Additionally, these meetings will also be used as planning sessions with the key stakeholders for business continuity and service resumption.

With the shift to Vendor’s Cloud, OSU has been able to build some degree of business resilience with the numerous applications which are built into public/vendor clouds. If there is a decision to fail over to the alternative DR site in City, State, various user offices will need to determine what data (from the point of failure) was no longer in the alternate site’s databases. As described earlier, OSU expects a fail-over from the production site within the City, State region to the City, State region would result in 15 minutes of data loss from the point the production environment failed. Each user office, consequently. would then need to analyze and resubmit those data changes.

**Addendum A**

**Network Topology**

**REDACTED**

**Addendum B**

**REDACTED**

**Addendum C**

For the most recent version of this addendum, please go to: [website](https://beav.es/imt-doc)

**Oregon State University | Information and Technology**

**Communications Response to Major Service Affecting Outages**

**Revision: April 2019 |**

# Purpose

IT and our campus IT partners understand that, despite our best efforts, service-impacting outages will occur. In some cases, these outages raise to the level of **Major** where the normal daily functioning of the University is negatively impacted. We wish to be well positioned with a plan for how to identify these **Major** outages, communicate the outage, plan our response, mitigate the affected pieces, and then recover from the outage.

# IMT Tiers

* **Tier 1:** NAMES
* **Tier 2:** NAMES

# Major Service Affecting Outage Examples

* Wide-spread network outage (wired or wireless)
* offline
* Canvas offline
* Central authentication offline/DNS
* Microsoft Exchange (employee email) off-line
* Web publishing for all of campus
* Hosted software applications that are in use by a broad group of the OSU community

# Key Personnel Assignment Definitions

1. Incident Commander (IC): responsible for the overall response to the outage, coordination of key personnel, and reporting to campus-level administrators.
2. Operations Chief (Ops): lead engineer responsible for the technical investigation and response to the outage.
3. Communication Lead (Comm-L): person assigned the responsibility of communicating to campus stakeholders that we have an outage, receiving updates from Ops, updating stakeholders on the progress of the outage, and providing a communication at resolution of the outage.
4. Incident Management Team (IMT): pre-planned group of individuals responsible for taking the lead on communication to campus during an outage.
5. Technical Staff Responsible for Service Operations: staff with day-to-day operational responsibilities for one or more IS services who is formally listed as or informally considered as primary person responsible for keeping service running.

*Note: At the beginning of an outage, IC and Comm-L could be the same individual. As an outage progresses, these tasks could be split.*

# Lifecycle of a Major Outage

1. Technical Staff Responsible for Service Operations (or designated on-call person) determines that a Major service impacting outage is occurring. **This determination includes the assessment that students, faculty, or staff are unable to complete their normal work due to the impact of the outage.** This assessment should consider scope that is campus wide (direct or indirect impact), and an on-going duration that is long enough to require alternative arrangements be made to complete work.
2. IT Staff report outage to supervisor, supervisor confirms Major assessment and escalates to any IMT member. If Major assessment is not confirmed, supervisor has discretion on response but is encouraged to notify IMT by non-emergency means as informational ([oregonstate.edu](mailto:is-imt@lists.oregonstate.edu)). If supervisor is not available, IT Staff report outage to on-call person for NOC, SIG, SSG or directly to any IMT member for which they have contact information. A default means of contacting someone on-call is to call 541-737-HELP option 2; it will page the NOC team. [Need to clean up mechanism: this number is not well advertised, and the phone tree is confusing.]
3. IMT member sends notice to NAME reporting the outage. **Note: it is important that the sender of any messages within SOFTWARE identify themselves by name and include the best number to reach them by.**
   1. For the first message, use NAME
   2. For the second message and all following, use NAME-B (proposed)
4. The IMT selects internally which member is available to take the IC and Comm-L position. The IMT communicates via a SOFTWARE group named **NAME** stating who will be IC/Comm-L.
5. IC/Comm-L designates Operations Chief (Ops) and establishes appropriate internal communication channels (slack, google hangouts, telephone conference, formal Incident Command Post, etc.).
6. The IC/Comm-L gets a briefing from Ops as to the scope of the outage and immediately begins communication. The initial communication to campus is intended to be brief and lacking in full detail - along the lines of “We are getting reports of a network outage beginning at around 10am today. We are investigating this and will post information as soon as it is known.” This communication will be sent to:
   1. Software list **Outages**, encompassing:
      1. IS Twitter feed [done]
      2. OSU social media network (Facebook, Twitter, etc.)
      3. Campus-wide IT Pros email list: [@oregonstate.edu](mailto:it.pros@oregonstate.edu) [done]
      4. Campus-wide Outages email list: [@lists.oregonstate.edu](mailto:outages@lists.oregonstate.edu) [done]
      5. Software contacts for individuals on Outages list? Group thinks yes, invite people to opt in.
      6. IT directors/managers university-wide via OSU email address and personal email address. [WILL BE COVERED WHEN THEY SUBSCRIBE TO SOFTWARE OUTAGES LIST]
      7. Posted to outage blog [COVERED BY OUTAGES LIST]
   2. When available, notified through a mobile application.
7. In all communication, details will be given as to which audiences are being communicated to.
8. As soon as scope is known, the same lists will be notified of the nature of the outage, and *if known*, the expected recovery window and the confidence level in this information. For example, “a piece of firewall hardware has failed. Repair is underway and we are cautiously optimistic that service will be restored by 10:30am.”
   1. If scope is not known within one hour, an update message will post stating that investigation is underway, and scope/recovery are not yet known.
   2. The same lists will be used for this communication.
9. Communications will repeat on the following schedule until the problem is fixed:
   1. Network - one hour
   2. Canvas - one hour
   3. Email - one hour
   4. - two hours

**Note: Some outages may require a *high-touch* method of communication with customers. Refer to Template 2a and 2b for more information.**

1. If the recovery is going to take an extended period, a more formal response team will be put in place. This response team will take over communications from a designated Incident Command Post (ICP). All IMT members will be informed of this change.
2. When the problem is resolved, a message will post to the same lists with:
   1. Outage period
   2. What happened (brief, non-technical version) and what services were affected
   3. Recovery confidence (likelihood of a repeat)
   4. Any pertinent user information, e.g., no email was lost, VOIP phones may need to be rebooted
   5. Contact info for follow-up problems
   6. Where the message is being posted, specifically whether a broader campus-wide communication will occur.

# Templates

## **Outage notice - within the first five minutes**

* 1. Time
  2. Nature of problem report
  3. Signature or contact information
  4. Where this notice was posted a
  5. Example: “At around 8am we began receiving notices that people are unable to login to . We are investigating the problem and will post more information as soon as possible. This message is posted to outages, -outages, acug, itpros, IS twitter feed, OSU IT Facebook, and twitter feeds.” NAME, IT- IT
  6. *Short Example:* OSU is experiencing issues. Staff are investigating. More details via email. END.

## **Status update**

For the status update, there are two options. Option A is a standard email every 1-2 hours, while Option B is a conference call with key customers of the service.

1. **Standard Email Communication**
   1. Time
   2. Nature of problem
   3. Diagnostic update
   4. Confidence level
   5. Contact or signature
   6. Where this notice was posted
   7. Example: “At 8am we began receiving notices that people are unable to login to . It appears that a process hung, and is being restarted and should be online within the hour. We are cautiously optimistic that this will fix the problem. This message is posted to outages, -outages, IS twitter feed, OSU IT Facebook, and twitter feeds.”
   8. *Short Example: OSU issues; fix is in the works. ETA for service restore is 1030a. More details via email. END.*
2. **Conference Call with Customers**
   1. Phone Number:
   2. Conference ID: XXX, followed by the # sign.

## **Recovery notice**

* 1. Time
  2. Nature of problem
  3. Resolution
  4. Confidence level
  5. Regrets
  6. Contact or signature
  7. Where this notice was posted
  8. Example: “ was unavailable from 8am-8:37 on Tuesday, November 1 due to a stalled process. has been returned to service and we do not anticipate any additional outages. We regret the disruption to service and thank you for your patience. Any lingering issues should be addressed to the OSU Service Desk, XXX, or at XXX. This message is posted to outages, -outages, IS “X” (formerly known as Twitter) feed, and the OSU IT Facebook page.”
  9. *Short Example: OSU issue is resolved. More details via email. END.*

# Reference

Sign up for OUTAGES SOFTWARE notification:

https://oregonstate.edu/alerts/osu-alert-portal

IS IMT listserv:

[@lists.oregonstate.edu](mailto:is-imt@lists.oregonstate.edu)

Outages list:

[@lists.oregonstate.edu](mailto:outages@lists.oregonstate.edu)

IT list:

[@oregonstate.edu](mailto:it.pros@oregonstate.edu)

SOFTWARE login:

[URL](https://www.getrave.com/login/oregonstate)

SOFTWARE login in case of DNS failure:

[IP](https://75.98.95.163/) Address

SOFTWARE login in case of DNS AND CAS failure (requires a local SOFTWARE password be set):

[URL](https://75.98.95.163/elogin.do)

# Emergency Contact List

* Use [this document](https://oregonstateuniversity.sharepoint.com/:x:/s/ISExec/EamvCLsk2hFHpJallvZYXq4BOQegz2BlqytlGIx0Ydl5Hg?e=MnMzGX) to access **emergency** contact information for key ITpersonal. Do not use this document for any other purpose and do not share outside of the organization.

# ICP (War Room)

* **Online ICP:**
  + If Auth **is** working and Zoom/MS Teams can be accessed normally:
    - Comms Lead creates Zoom/MS Teams room using personal account and share the link **and** phone number to the IMT Software group.
* **Offline ICP:**

1. Linc
2. JSB

# Inform Lists:

* List01
  + Chief Officers, Executives, Dean
* List02
  + Top Administrators - Academic & Research
* List03
  + Top Administrators - Administration
* List04
  + N/A
* List05
  + N/A
* List06
  + Classified Staff
* List07
  + Professional Faculty
* List08
  + Instructors, Research Associates/Assistants
* List09
  + Professors, Associate/Assistant Professors
* List10
  + Academic Advisors
* List11
  + Office Managers, Executive Assistants
* List12
  + Academic Wage & Other Misc
* List13
  + Emeritus

*6, 7, 8, 9 and 12 for “all employees”*

# Additional Considerations

*Communicator Awareness*

* Make key campus communicators aware of outages. Colin Huber, et al

*Classification of outages*

* *Pending creation of outage matrix*

*Anatomy of IMT first message*

* Name of activator
* What do you need from the IMT? FYI? Advise? Need roles filled?

*Policy for short duration/minor outages (High confidence)*

* *When to send campus-wide email versus smaller audience*

**Periodic Review**

This document & process should be reviewed on an annual basis to ensure the process is still effective and the people/roles involved are appropriate.

**Addendum D**

**REDACTED**

**Addendum E**

**IT Emergency Contact Information**

**REDACTED**

**How to contact individuals on the emergency contact list (above): The cell phone information for all the relevant individuals is stored in OSU’s sharepoint.**

**Emergency contact list:**

**To trigger communications to these teams OSU utilizes the Alert Portal software (Software). This portal can be accessed via the following link: The Alert Portal is managed by:**

**OSU’s Emergency Preparedness Manager**

**Alert Portal (Software) Emergency IT Alerts:** **NAME**. These alert lists within SOFTWARE allow simultaneous messages to go out to individuals on those lists via email, text message, and personal cell phone/voicemail. Use these alert lists to coordinate/communicate with key incident management response teams.

**Link Oregon:** If the issue is pertinent to Link Oregon. Link Oregon’s website:

**Addendum F**

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Continuity-Disaster Recovery Plan**  **Test/Maintenance Log** | | | |
| **Date** | **Description of Plan Update or Test** | **Result** | **Responsible Person** |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |
| DATE | EVENT | Success | NAME |

**Addendum G**

**Vendor Cloud Backups**

**On-Premise Backups:** OSU has a few services which are still on premise. Vendor service (a Microsoft-based solution), the Vendor transcript ordering service. All these services are backed up to the Amazon Web Services Simple storage system (S3) site.

**Vendor Cloud Backups:** OSU takes advantage of Vendor’s Cloud (Cloud) Backup service for all the database, operating system, and software file system backups, which are in the Cloud.

**OS, Database/Archive Logs, and Software file systems:** The file systems for the Vendor Linux operating systems (OS), the Vendor Relational Database Management System (RDBMS) database/archive logs, and application files for Administrative Software (and other accompany administrative software) are backed using Cloud’s Console for both the Vendor database backup service and volume backups. All three backups are encrypted.

**Operating systems backups:** Operating systems are run from an Vendor block storage service which are backed up each night at 12am (midnight). The cadence for these backups and retention of the backups are:

* Daily – incremental, and kept for one week
* Weekly – full, and kept for four weeks
* Monthly – full, and kept for 11 months
* Annual – full, and kept for five years

**File system backups**: Software file systems are run from a SAN storage service which are backed up each night at 11:30pm. These include most of the files. The cadence for these backups and retention of the backups (aka snapshots) are:

* Daily Snapshot – daily for 24 days, and are cycled out daily on the 25th day. This is equivalent to the 30 days of database backups.
* Weekly Snapshot – every seventh day, and kept for 12 weeks
* Monthly Snapshot – every month, and dept for 11 months
* Annual Snapshot – every year, and kept for five years

**Database backups**

All Vendor database backups are stored in an object storage bucket owned/operated by Vendor. All database backups are hot full (Level 0) and incremental (Level 1) and are kept for 30 days. Hot means the backups are taken while the DB is running. Incrementals represent the deltas from the previous day. OSU does a full hot backup on a weekend day (Friday night/Sat morning between 10pm-12 midnight) and hot incrementals (also 10pm-12 midnight) for the rest of the week. Archive logs which manage the individual transaction processing (~250GB) are backed up every 60 minutes and kept 41 days. This allows OSU to be able to restore the data in the Vendor database to a specific point-in-time or to the “current” point-in-time within the previous 41 days.

**Location:** Vendor stores OSU’s backups on a separate infrastructure than the production site infrastructure. The backup infrastructure exists across three of Vendor’s second-generation data centers in City, State. OSU, however, also backs up its backups to Vendor’s City, State site.