

EL PASO COMMUNITY COLLEGE PROCEDURE

Business Continuity Planning

APPROVED:

REVISED:

AUTHORIZING BOARD POLICY: 2.05.1

OBJECTIVE: This procedure was written to guide El Paso Community College (EPCC) in writing a department's Business Continuity Plan which guides the reconstitution of departmental capacity after a service disruption. The Vice President for Information Technology/Chief Technology Officer has overall responsibility for this procedure.

El Paso Community College has an obligation to protect and provide for our students, faculty, staff and visitors in the event of a major interruption of our mission and operations. Further, the College recognizes that these obligations extend to a responsibility for each department within EPCC to be able to meet its individual obligations. These include the ability to provide the services expected of them and to carry out functions critical to the mission of the College should an event which interrupts the normal course of operations occur. Failure to have an adequate continuity plan could lead to unnecessary injury or loss of life, financial disaster, interruptions of academic classes, and delays in completing other mission critical activities.

All departments are encouraged to have reasonable business continuity plans to ensure continuation of programs and services in the event of a major disruption of operations. Departments that are critical to carrying out the EPCC mission are required to have business continuity plans, and to exercise and update their plans regularly. The Office of the Vice President for Information Technology/Chief Technology Officer shall assist in the coordination of the continuity planning process for critical departments. The Office of the Associate Vice President for Auxiliary Services should be available to assist departments in determining what space, equipment, and services will be available within the College and to make the planning process more efficient.

A plan for business continuity shall contain clear strategies and procedures needed to continue operations and execute a recovery in the event of an interruption that compromises the ability of the department to carry out its critical functions. The determination that an interruption has occurred may be made by the individual department manager, its administrator or by the College Administration. Departments may establish "levels" of interruption and appropriate interruption response.

If any department with a critical mission depends on suppliers, other EPCC departments or external Service Bureaus or vendors to provide its critical functions, those suppliers or departments must also have a continuity plan.

Annually, on or before August 31, each department with critical mission functions must submit to the Office of the Vice President for Information Technology/Chief Technology Officer certification that the department has reviewed, exercised and updated its plan.

PROCEDURE:

I. Who Should Know This Procedure

Beside the Office of the President, the Office of the Executive Assistant to the President, Vice Presidents, Associate Vice Presidents, Deans, and Directors/Budget Heads/Instructional Coordinators, there are other staff and groups that should know of this procedure. The EPCC Police Department, Information Technology and all those with a role in business continuity of any department should be aware of this procedure and the Business Continuity Plan for their area of responsibility.

II. Related Information

Pertinent references to other policies/procedures (if any) will go here.

III. Contacts

Subject	contact	phone
EPCC Police Department	Dispatch Operator	915-831-2200
Communications (voice)	Telecommunications Department	915-831-2000
General Questions/Plan Development and Review	Information Security Office	915-831-6312
Information Technology	IT Help Desk	915-831-6440

IV. Definitions

A. Mission Critical Functions: Processes or applications that are essential to the ability of the College to provide its services or perform its activities safely and effectively. The Administrator for a department is responsible for determining if the applications or processes owned by a department or program fall into one of the following categories.

1. Safety and Security: Activities needed to support a safe and secure environment for students, faculty, staff, patients, the visiting public and surrounding community. Police, Fire and Ambulance services as well as adequate lighting and usable facilities that are in good condition and safe to occupy are necessary for the continuation of all EPCC activities. Access to and egress from campus and classrooms as well as maintenance of

equipment, materials and facilities for the conduct of day to day operations. Safe handling and proper disposal of toxic substances, biologically hazardous materials, and radioactive materials.

2. Learning, Education and Research: Activities that carry out or directly support the academic mission of EPCC. For example, student support services (admissions, registration, etc.), lecture & study, grant-funded programs, graduation.

3. Business Support Services: Activities that allow EPCC to maintain necessary business operations, safeguard assets, and ensure the financial viability of the College. Examples include: payroll, revenue collection, accounts payable, investing, and financial reporting. If so, they are considered to be "critical" and must be covered by a Business Continuity Plan.

If so, they are considered to be "critical" and must be covered by an Operational Continuity Plan.

Critical Operating Units

Operating units defined as critical include the following:

Critical Operating Unit	Vice Presidential Unit
1. Facilities Management	Executive Assistant to the President
2. University Police Department	Student Services
3. Networking & Telecommunications	VP for IT/CTO
4. IT Computer Operations	VP for IT/CTO
5. Personnel - Employee Benefits	Personnel
6. Personnel – Class & Comp	Personnel
7. Personnel HRMS	Personnel
8. Comptroller	Sr VP for Systems Administration
9. Registrar	Sr VP for Systems Administration /OIT
10. Budget & Finance	Associate VP for Budget & Fin Svcs

B. Business Continuity Plan: A plan that clarifies strategies and documents the procedures needed to continue operations and execute a recovery of critical applications or processes in the event of an interruption. It also includes procedures used to exercise recovery capabilities.

C. Back-up Agreement: Written agreement between two parties that identifies and specifies the responsibilities of the parties as they relate to continuity and recovery in the event of a business interruption. If the agreement is with non-EPCC entities, it must be in contractual form and it must be approved by the

EPCC Counsel. A copy of all Back-up agreements must be included in the department's Business Continuity Plan.

- D. Department:** Any department or division under the business control of an Associate Vice President, a Dean, Director, or Department Head having budget authority.
- E. Department Manager:** The Associate Vice President, Dean, Director, or Department Head in business control of a department.
- F. Service Bureau or external vendor:** Any agency or department that provides services to multiple departments (e.g., police, Information Technology service areas, Center for Instructional Telecommunications, etc.). Service Bureaus may or may not be College based.
- G. Interruption / Disaster:** Any occurrence that compromises the ability of the department to carry out its critical functions. The determination that an interruption / disaster has occurred may be made by the individual Administrator or by EPCC Administration. Departments may establish "levels" of interruption /disaster and of interruption / disaster response.

V. Responsibilities

- A. Vice President for Information Technology/CTO:** Alert the President and/or appropriate senior staff when departmental Business Continuity Plan has not been developed. Report on the status of overall College Continuity planning. Maintain accuracy of the procedure. Annually report on the Planning that has been developed and exercised.
- B. Associate Vice President for Auxiliary Services:** Publish and distribute Resources to assist the departmental planning function.
- C. Business Continuity Coordinator (BCC):** Serves as a focal point for business continuity planning within the department. The BCC and the functional responsibilities of the BCC will be determined by the department's Administrator or Budget Head.
- D. President:** When alerted by the Vice President for Information Technology/CTO, assure that departmental Business Continuity Plans are developed.
- E. Recovery Teams:** Implement the Business Continuity Plans for all departments, as needed.
- F. Administrator:** The Administrator is responsible for:

1. determining if the applications or processes owned by a department fall into one of the mission critical categories
2. designating the functional responsibilities of the Business Continuity Coordinator
3. reviewing the plan annually and exercising objectives and results
4. updating and maintaining the plan
5. evaluating the impact of changes within the department and their impact on the department's ability to recover from a serious business interruption
6. responsible for creating the plan, exercising the plan and training employees to be proficient at their roles within the plan.

VI. General Provisions

Each El Paso Community College (EPCC) Administrator must determine which of the department's processes or applications are mission critical. The current departmental mission statement, goals and objectives should be used as a guide, but are not limiting.

Each EPCC Administrator along with their designated Operational Continuity Coordinator must develop a Business Continuity Plan (BCP) that defines the steps necessary to resume mission critical activities in the event of an interruption. They must also develop the procedures for performing these activities. Any plans or procedures must take into account the possibility that an EPCC-wide disaster may affect multiple departments. If any department depends on suppliers, other departments or outside Service Bureaus to provide its critical functions, those suppliers or departments must also have a continuity plan. Copies of back-up agreements between departments must also be included in the plan, as must agreements with non-EPCC based Service Bureaus and suppliers.

In the event that limited resources and alternatives require that the priority for the recovery of one department be ranked against another department, the determination of this priority will be made by the President or his designated representative.

A. Process: For each of the mission critical processes or applications identified, incorporate the following into the Business Continuity Plan:

1. Mission Critical Processes or Applications: Identify processes applications which fall into any of the following categories:

- Safety and Security
- Learning, Education and Research
- Business Support Services

2. **Risks/Hazard Analysis:** Identify risks and/or hazards that might reasonably pose a threat to the department's ability to function. Identify existing and /or easily implemented controls to avoid these risks and hazards.
3. **Time to Failure:** Identify how long the department can function without normal support tools (e.g., business records, computers, telephones, etc.)
4. **Operating Level:** Determine the minimum levels of operation at which the department will function during the disaster and the recovery process.
5. **Recovery of Resources/Information:** Determine how the department will identify which resources, information, transactions, documents, data, etc. have been lost due to the disaster and how they will recover and/or reprocess the items identified.
6. **Recovery Time:** Determine time frames for the full recovery of critical functions.

B. Operational Continuity and Recovery Strategy: Each department must develop a documented continuity and recovery strategy that enables the department to continue to perform critical functions and/or provide services within a pre-defined time frame. The type and level of service to be provided within this time frame and the method of recovery must be defined. Take the following actions to implement the strategy:

- Back up all critical files (regardless of media)
- Document the location of the off site storage in the plan
- Identify a recovery team consisting of all persons responsible for executing the Business Continuity Plan
- Determine when the Business Continuity Plan needs to be activated and identify who within the Department is authorized to implement the plan
- Identify all persons with copies of Business Continuity Plans and have them available for review. Store at least one current copy in an off site facility with immediate availability
- Maintain the list of resources, vendors, Service Bureaus etc. with which the department has written back up agreements for the provision of services, equipment, etc to be used in the event of a disaster
- Establish procedures for contacting, appropriate College department and EPCC and non-EPCC suppliers/Service Bureaus in the event of an interruption in operations

- Establish procedures for return to full, normal operations of the department including recovery of non-critical functions.

C. Documentation & Record Keeping

Include printed copies of all back-up agreements in the plan.

If you use a Service Bureau / supplier to provide support for critical functions, ensure that the Service Bureau / Supplier has a continuity plan which will protect the College in the event the Service Bureau / Supplier suffers an interruption. Include verification of Service Bureau / supplier continuity plans with your plan.

Document procedures for notifying staff with continuity responsibilities in the event of an interruption. Develop and maintain a list of recovery responsibilities and the staff assigned to each responsibility. For each responsible staff member there must also be an alternate staff member. The list must contain, at a minimum, the following information:

- The names of the employee and alternate for each continuity responsibility
- Business and home phone numbers for each employee and alternate
- General recovery responsibilities of the staff member and alternate
- Procedures required to support the recovery strategy that are not documented elsewhere must be documented in the recovery plan
- Documentation required to support restoration of critical functions must be kept current and must be stored in an off site facility with immediate availability

NOTE: Standards and Procedures manuals do not need to be replicated in the Business Continuity Plan, but the manuals must be readily available at accessible locations.

D. Exercising:

Business Continuity Plans must be exercised by the Administrator at least once per year. A successful exercise will include the following:

- Identifying exercise objectives
- Conducting exercises using the Business Continuity Plan
- Evaluating exercise results and, if needed, making appropriate changes to the plan and re-exercising to ensure that objectives are met

- Documentation of exercise results and the steps proposed to correct any problems

E. Training:

1. Administrators will assure that training (on the use of the plan) is provided on an on-going basis to all personnel of the department in order to ensure that all staff is adequately trained to fulfill their responsibilities in support of the recovery process.
2. Training must include familiarity with and a working knowledge of the department's Business Continuity Plan.
3. Training for new employees should be carried out within 30 days of beginning employment.

F. Reporting:

A letter certifying the level of achievement for each BCP objective exercised must be sent to the responsible Vice President and to the Vice President for Information Technology/CTO. The letter should also report the result of the annual review of the BCP.

Business Continuity Plans must be reviewed by the Administrator once per year. In particular, the Administrator must assure that:

- Critical functions have been identified
- Continuity and recovery strategies are in place
- Documentation for the plan is current
- Minimum levels of required operation and recovery time frames have been set
- Exercising of the plan has been completed during the last 12 months
- Certification of the annual review must be sent to the Vice President for Information Technology/Chief Technology Officer and maintained by the Administrator

The plan and associated documents must be available for review by the Office of the Vice President for Information Technology/Chief Technology Officer.

G. Administration of the Plan: Planning and plan maintenance is the responsibility of the Administrator.

1. **Plan Maintenance:** Administrators must evaluate the impact of changes within the department and communicate any changes to all persons holding copies of the plan. All changes, after the

initial effective date, must be attached and then become a part of the document.

- 2. Unique Needs:** List any special needs that are unique to your operations such as special equipment, unique skills needed to recover, etc. The needs, should funding be required, should be detailed in the BCP and in the departmental budget request for the next fiscal year.
- 3. Amendments:** All amendments must be recorded and appended to the plan.
- 4. Forms/Instructions:** In support of this procedure, the following forms and instructions are included:
[Letter Certifying Compliance with Exercising of Business Continuity Plan](#) - PDF Format
- 5. Appendices:** In support of this procedure, the following appendices are included:
[Appendix A - Processes That May Require Business Continuity](#)