المملكة العربية السعودية
وزارة التعليم العالي
جامعة الملك سعود
كلية التربية
قسم الإدارة التربوية

ترجمة المقال ٢ بعنوان:
نظم المعلومات الإدارية

إعداد:

الطالبة/ أريج مكي الجهني
الرقم الجامعي : ٤٢٩٢٠٤١٣١

إشراف/

د.امتثال أحمد السقا

متطلب جزئي لمقرر تطبيقات الحاسب في الإدارة التربوية (٥٣٦إدت)
الفصل الدراسي الثاني١٤٣٠/١٤٣١هـ

عنوان المقال :

نــظــم المـعـلـومـــات الإداريـــــــــــة

سبب الاختيار :

ارتباطه بشكل مباشر **بالمقرر بالمحور الثالث على وجه التحديد نظم المعلومات الادارية واهمية المعلومات وسمات المعلومات واحتوائه على معلومات حديثة ومتنوعة .**

تلخيص المقال:

يقع البحث في أكثر من ٢٠ صفحه ، ويتناول موضوع نظم المعلومات الإدارية بالتفصيل من ناحية تعريفه وسياسة المعلوماتِ الإداريةِ ووظائف النظم المعلومات الإدارية ، ويتطرق إلى تعريف فريق موارد إدارة البيانات ، كذلك يتحدث عن دور المشاريع الخاصة وتصنيف البيانات فهناك بيانات تتسم بالخصوصية وهناك من تتسم بالحساسية والنوع الثالث البيانات الغير مقيدة ، ثم يستعرض البحث سبع مهام أساسية في نظم المعلومات الإدارية وهي سياسة امن البيانات وحماية البيانات ، ولجان الحوسبة الإدارية وفريقها والمدققين الداخليين وحوسبة الخدمات وأمن المعلومات والمراقبين العامين ، كما يختتم البحث بالحديث عن تغيرات النظام واستعراض أهم المصطلحات المتناولة في البحث .

أولاً : تعريف نظم المعلومات الإدارية :

المعلومات الإدارية هي أي بيانات تتعلق بالأعمال التي تكون مؤسسة التعليم العالي. وعرفت ولاية جاكسون المعلومات الإدارية كما يلي هي تكوين قاعدة بيانات لتكون مصدر جامعي الأمر الذي يتطلب الإدارة الصحيحة من أجل السماح للتخطيط الفعال واتخاذ القرارات ولإجراء العمل في الوقت المناسب وبأسلوب فعال.

سياسة المعلومات الإدارية :

المعلومات الإدارية لا تتضمن مقتنيات المكتبات أو البحوث أو مذكرات تعليمية إلاّ إن كانت تحتوي على المعلومات التي تتعلق بوظيفة العمل. مثل هذه الوظائف تشمل (ولكن ليس محصورة إلى) المالية، وشؤون الموظفين، الطلاب، الخريجين، الاتصالات، وبيانات الموارد الفيزيائية. وهي تشمل البيانات التي حفظت في الإدارات ومستوى المكاتب، بغض النظر عن أجهزةِ الإعلام التي تسكن فيها ، ولاية جاكسون احتفظت بملكية جميع المعلومات الإدارية التي تم إنشاؤها أو تعديلها من قبل موظفيها كجزء من مهام وظائفهم.

وظائف مجموعةِ أنظمةِ المعلوماتِ الإداريةِ

مجموعة أنظمة المعلومات الإدارية توفر حلول تكنولوجيا المعلومات والخدمات التي تعزز المهمة الأكاديمية وعملية عمل كلية الزراعة وعلوم الحياة. التشكيلة الواسعة للوظائف تتضمن:

- عملية عمل التحليل
- تصميم النظام
- البحث التقني والتحليل
- تطوير تطبيقات جديدة
- تكامل الأنظمة
- إدارة قاعدةِ البيانات لقواعدِ البيانات المتعدّدةِ
- برمجة الأنظمة
- دعم وصيانة الأنظمة القائمة
- إدارة المشاريع

فريق موارد إدارة البيانات (DMRT)

إن إدارة البيانات وفريق الموارد مسؤولين عن إنشاء أنظمة فعالة لإدارة البيانات لاستخدامها في المالية الحالية، وتطوير تقرير إداري، والانتشار والصيانة التي تتوافق مع حاجات المؤسسات والأهداف.

المشاريع الخاصة:مجموعة المشاريع الخاصة تزود التوجيه التقني على المشاريع المعقدة، وتزود المساهمة والتوجيه على الاتجاهات التقنية، ويصوغ البنى التحتية والهندسة المعمارية في دعم عمل سي أي إل إس.

يمكن أن تصنف المعلومات الإدارية إلى ثلاثة مستويات من الحماية لأغراض أمنية:

١- **المعلومات الخصوصية :** وهي المعلومات التي تحتاج إلى مستوى عال من الحماية بسبب الخطر ومقدار الخسارة أو الأضرار التي يمكن أن تنجم عن كشف أو تعديل أو تدمير البيانات. وهذا يشمل المعلومات التي ساء استخدامها أو الكشف عنها يمكن أن يؤثر سلبياً على العمل .

٢- **المعلومات الحساسة :** وهي المعلومات التي تحتاج إلى بعض من مستويات الحماية لأن الكشف عنها غير مرخص، والتعديل أو التدمير قد يسبب أضرار إلى العمل .

٣- **المعلومات الغير مقيدة :** وهي المعلومات التي يمكن أن تُجعل متوفرة عموماً ضمن وما بعد الجامعة.

نستعرض الآن بشكل موجز المهام أساسية في نظم المعلومات الإدارية :

وهي سياسة امن البيانات وحماية البيانات ، ولجان الحوسبة الإدارية وفريقها والمدققين الداخليين وحوسبة الخدمات وأمن المعلومات والمراقبين العامين .

أولاً : سياسة امن البيانات:

إن المعلومات تتطلب نوع من المسؤولية والسرية والفشل في حماية هذه المصادر قد يؤدي إلى إجراءات تأديبية تؤخذ ضد المستخدم.

دور الموظفين :

بالإضافة إلى وجود الموظفين الدائمين ، مصطلح موظف يشمل الموظفين المؤقتين، المستخدمين الطلاب، والاستشاريين، والمتطوعين، المساعدين.

المسؤوليات :

المستخدمون مسئولون عن أمن البيانات الإدارية.

ومن مسؤوليات المستخدم :

- الامتناع من الدخول واستخدام المعلومات في الطرق الغير مرخصة المستخدمون الذين يحاولون الدخول الغير مرخص لهويات دخول الحاسوب الإداري يخضعون لإجراءات تأديبية.
- إتباع الإجراءات اللازمة لمخزن البيانات
- إتباع الإجراءات للتخلص من البيانات
- حماية البيانات من دخول غير موثوق : ومنها عدم الإفصاح بكلمة السر لدخول النظام حتى مع المشرفين و تغيير كلمة السر كل ٩٠ يوم حتى لو لم يجبر النظام لذلك والإبلاغ عن أي اختراق أمني

المشرفون :

يستخدم مصطلح "مشرف في هذا الدليل بحساسية عامة لدمج ليس فقط الناس الذين وظيفة عملهم تعرف لتشمل الإشراف على الموظفين، ولكن أيضاً لتوجيه الناس الذين يديرون عمل الآخرين. مثل هذه العناوين كمشرف، مدير، قائد، رئيس، رئيس قسم، عميد، ونائب الرئيس يستخدموا رسمياً ليدلوا على المشرف بشكل عام .

المسؤوليات :

وهي مسؤولية المشرفين للحفاظ على مستوى عالي من الأمن في موقع العمل. المشرفون يتحملون المسؤولية لإبلاغ موظفيهم الأسلوب الصحيح لمعالجة المعلومات الإدارية، لتقييم فعالية هذه الإجراءات، ويوصوا بتغيرات لتحسين هذه الحماية. وبالإضافة إلى مسؤوليات الأمن

المطبقة على جميع العاملين، والمشرفين لديهم مسؤوليات تتعلق بأمن البيانات على النحو المبين أدناه:

- مراجعة دخول موظفيهم
- يضمن بأن المستخدمون امتثلوا للسياسات الأمنية والإجراءات
- استخدام مراقب لتحديد المشكلة
- إيقاف الدخول عندما الموظف يترك القسم

الرئيس/ رئيس القسم

تعريف

مصطلح رئيس/ رئيس قسم يستخدم ليدل على مدير الإدارة، أكاديمي أو البحث ضمن وحدة في الجامعة. هذا الشخص لدية مسؤولية مالية للقسم تتضمن تحضير الميزانيات ومراقبة التصرف. الرئيس/ رئيس القسم يبلغ مباشرة إلى مدير كبير.

المسؤوليات:

الرئيس/ رئيس القسم مسؤول عن تأسيس بيئة أمنة مطلعة على البيانات تستخدم بالقسم. هو يضع إجراءات تتعلق بأمن البيانات ودعم هذه الإجراءات بتوزيع الأموال.

الرئيس/ رئيس القسم يجب أن يراجع إجراءات المكاتب على الأقل على قاعدة سنوية وعمل تحديثات للرد على التغيرات في السياسات والتقنية.يجب أن تتوقع الميزانيات السنوية الحاجة لمصادر التمويل لحماية معلومات إدارية عينت في القسم. بالإضافة إلى مسؤوليات الأمن الملائمة لكل المستخدمين والمشرفين، الرئيس/ رئيس القسم لديه المسؤوليات التالية بخصوص أمن البيانات:

- ترجمة السياسات إلى إجراءات المكاتب
  - يجب تثبيت برنامج حماية من الفيروسات على كل الحاسبات الصغرى التي تحفظ المعلومات الإدارية لتحمي البيانات من التشويه أو الدمار.
  - رؤساء/ رؤساء القسم يجب أن يضمنوا بأن صيانة الحاسوب اتخذت في سلوك لحماية سرية البيانات المخزنة في النظام.
    - يزود بالمصادر لتنفيذ الإجراءات
  - عندما لم يعد هناك حاجة لمعلومات إدارية غير إلكترونية في القسم، يجب أن تكون الآليات للتخلص من البيانات متوفرة. يجب أن تمزق المعلومات السرية في القسم أو تنقل بشكل أمن لتمزق أو تحرق بوسيلة صحيحة.
  - المعلومات الإدارية الحساسة أو الحرجة تحفّظ على الحاسوبات الصغرى يجب أن تبقى ضمن تقسيم إلكتروني الذي يتطلب كلمة سر للتمكن من الوصول.
    - تحديد حساسية البيانات الغير مركزية التي نشأت في القسم

ثانياً : **حماية مسؤولية البيانات**

حماة مسؤولية البيانات مسؤولون عن تأسيس تعليمات للإدارة وحماية هذه البيانات ولعمل التوصيات لتحسين توفر مصادر هذه الجامعة. كل حامي مسؤولية البيانات هو مسؤول عن مجموعة فرعية من المعلومات الإدارية الذي يحميها بالطرق التالية:

- الحفاظ على معرفة مفصلة للبيانات ضمن ثقتهم.
- إدارة نشاطات تتعلق بعمل المعلومات
- تطوير تعليمات لطلب الدخول
- مراجعة الطلبات لدخول إلى المعلومات الإدارية
- تعريف حساسية البيانات
- تطوير التعليمات للمعالجة الصحيحة من المعلومات الإدارية
- مراجعة المعلومات المستخدمة
- المساعدة في تطوير الممارسات الأمنية الموحدة
- المساعدة في التخطيط لاستئناف الأعمال

ثالثاً : **لجنة الحوسبة الإدارية**

تعريف

مصطلح "لجنة الحوسبة الإدارية" يشير إلى مجموعة ضباط يحددون الاتجاه، في النهاية ارتبطت السياسات بالحوسبة الإدارية. هؤلاء الضباط يتضمنوا الرئيس، نائب الرئيس لتقنية المعلومات، ونائب الرئيس للمالية أو ممثليهم المعينين.

المسؤوليات:

لجنة الحوسبة الإدارية لها مسؤولية لضمان حماية المعلومات الإدارية لولاية جاكسون، تأسيس السياسات والفلسفات للمعلومات وأمن البيانات وتخصيص مسؤوليات إلى مستخدمي الجامعة المختلفين لمساعدة اللجنة في هذه الأمور. مسئولياتهم فيما يتعلق بالمعلومات والأمن:

- مراجعة وتقييم الخطط لأنظمة المعلومات الإدارية
- مراجعة وتصديق السياسات
- مراجعة ضوابط الأمن
- توفير الوسائل لتطبيق السياسات
- تنفيذ السياسات
- توضيح وتفسير السياسات
- ضمان بأن تبقى السياسات على حالها

رابعاً : **المدققين الداخليين**

تعريف

يستخدم "مدقق داخلي" في هذا الدليل ليشير إلى مدقق الجامعة وأعضاء آخرين من موظفي التدقيق الداخلي. وهو غير قابل للتطبيق إذا لم يكن من مستخدمين ولاية جاكسون. يزود المدققين الداخليين وجهة نظر موضوعية ومستقلة إلى الجامعة على الأمن لمصادر معلوماته.

المسؤوليات:

بموجب دستور مدقق الجامعة، مدققين داخليين لولاية جاكسون هم مصدّقون لتحقيق دخول لكل الأنظمة والمعلومات الإدارية، ومسؤولون عن مساعدة المشرفين في تأدية واجباتهم بفعالية. بالإضافة إلى أن يكون موضوع سياسات أمن المعلومات قابل للتطبيق من قبل مستخدمين آخرين لولاية جاكسون، يجب على المدققين الداخليين لولاية جاكسون المصدق عليهم أن يلتزموا بتدقيق المعايير والرموز التي أسست من قبل مجموعات ملائمة مصدق عليها. في ممارسة واجباتهم المتعلقة بأمن المعلومات والمدققين الداخليين:

- تقييم الامتثال لسياسة أمن المعلومات والإجراءات ضمن أقسام الجامعة أثناء تدقيق عملي وإداري.
- تقييم فعالية إجراءات الأمن وسيطرة داخلية لدخول محدد إلى المعلومات الإدارية المخصصة وتحديد واقتراح التحسينات لمناطق الضعف.
- مراجعة آثار تدقيق الحسابات المزودة من قبل أنظمة تطبيق الأمن لتقييم إذا نشاط موثق بشكل كافي يسمح للأخطاء ويحدد الأخطاء، لتتبع مصدرها وتصحح.
- يساعد الإدارة في التحقيق في حوادث مشبوها لاختراق الأمن أو نشاط غير لائق.
- تزويد نصيحة على السيطرة الداخلية ذات العلاقة لتجديد الأنظمة لتكون متطورة أو تعتبر للشراء.

خامساً : **حوسبة الخدمات وموظف تقنية المعلومات**

المسؤوليات

حوسبة الخدمات وموظف تقنية المعلومات لديهم الخبرة والمسؤولية لحماية المعلومات الإدارية المقيمين على الحاسبة الإلكترونية للجامعة، شبكة، وخادمات محلية ويجب أن تستخدم هذه الخبرة في أخلاق المسؤولية لضمان سلامة البيانات وتوافر المعلومات. بسبب فرصتهم الكبيرة لدخول المعلومات الإدارية، موظف تقنية المعلومات وحوسبة الخدمات لدية مسؤوليات إضافية.

- التقيد باتفاق عدم الكشف عن القسم
- الحفاظ على البيانات والبرامج ضمن معايير مؤسسة
- توفير الأمن لأنظمة الحاسوب
- المساعدة بتطوير خطط بعيدة المدى

- التدريب والتشاور مع الحوسبة الإدارية
- المساعدة بتطوير خطط استئناف العمل

سادساً : **ضابط أمن المعلومات**

المسؤوليات:

ضابط أمن المعلومات مسؤول عن تأسيس ومراقبة الإجراءات لضمان بأن المعلومات الإدارية لولاية جاكسون حميت من دخول غير مصرح به، حميت من تعديل خاطئ ومتوفرة لدى مستخدمين موثقين بطريقة مناسبة لتمكينهم من أداء واجباتهم. متضمن في هذه المسؤوليات الضرورة ليكون الفني فصيح بالأنظمة الأمنية المختلفة تستخدم لحماية البيانات وللتعويض باستخدام الإجراءات، لأي عيوب لهذه الأنظمة. هذه المسؤوليات تتضمن التالي:

- تطوير وإبقاء إجراءات أمن فعالة
- اختبار وتوثيق أنظمة أمنية إدارية
- الاستشارة على القضايا الأمنية الداخلية
- تحضير واحتفاظ بسياسات أمن عامة وتعليمات
- تزويد المساعدة بتدريب الأمن
- مراجعة مخزن دخول البيانات

سابعاً : **مدراء هوية الدخول**

المسؤوليات

مدراء هوية الدخول هم مستخدمين ولاية جاكسون، لمن تضمن واجباتهم الإنشاء، الحذف، أو تعديل هويات الدخول أو صيانة هوية جداول الدخول التي تتحكم بالقدرة لعرض أو تحديث المعلومات الإدارية. بسبب مجال هذه القابلية، مسؤوليات إضافية خصصت لدخول هوية المدير كالتالي:

- المحافظة على توثيق كامل لكل التغييرات .
- تنفيذ دخول عرف من قبل حامي مسؤولية البيانات
- تعليق الدخول عندما ينتهي أو يحول المستخدم

أخيراَ تغيرات النظام :

- نظام الإنتاج

كل التغيرات التي اقترحت لبيئة الإنتاج يجب أن تصدق من قبل إدارة عالية المستوى. أي فرد أو مجموعة يتأثروا بهذه التغيرات يجب أن يبلغ عنها في كتابة سابقة للتغيرات التي اتخذت. يجب أن تصنع التغيرات في بيئة الاختبار ويثبتوا قبل أن يوضعوا إلى الإنتاج. تغيرات نظام التطبيق يجب أن تصدق من قبل ذلك حامي الأنظمة وعضو موظف مركز الحاسوب الذين هم صنعوا.

يصدق مرة واحدة، هذه التغيرات يجب أن تركب في بيئة الاختبار وأن تختبر من قبل موظفي مركز الحاسوب وجالية المستخدم قبل أن توضع إلى الإنتاج.

- اتصالات البيانات

التغيرات المقترحة إلى تركيبة شبكات الجامعة قبل أن تصدق من قبل إدارة مراكز الحاسوب قبل أن تصنع. كل التغيرات يجب أن تصنع أولاً في بيئة الاختبار حيث التغيرات تختبر وتحقق لتكون صحيحة من قبل شخص يطلب التغير وأعضاء موظفي تقنية المعلومات.

يتضح مما سبق أهمية امتلاك المنظمات بشكل عام والمنظمات التعليمية بشكل خاص لنظام خاص لإدارة المعلومات بها .

التعليق على المقال :

لقد غيرت الثورة الرقمية . المتمثلة في المعلومات والاتصالات . التي يشهدها العالم الآن الكثير من المفاهيم الإدارية ، فنجد أن معظم الدول المتقدمة تقنيا أصبحت تعتمد اعتمادا أساسيا في عملها على نظم المعلومات، وإدخال هذه التقنية في معظم الأجهزة الحكومية والخاصة، وعلى الأخص في الأجهزة الإدارية التي تقوم بتقديم الخدمات العامة للمواطنين، ومعظم تلك الأجهزة لها اتصال مباشر من خلال شبكات الحاسب. ولقد أدركت مختلف بلدان العالم الثالث بما فيها الدول العربية أهمية نظم المعلومات، ودخلت الكثير منها بدرجات متفاوتة هذا المجال لكي تشارك في مجال الاستفادة العلمية والتربوية.

ونظم المعلومات هي نظم آلية تتكون من مجموعة من المكونات التي تستخدم للقيام باستقبال موارد البيانات، وتحويلها إلى منتجات معلوماتية .

وتلعب المعلومات دورا هاما في تحقيق التكامل بين المتغيرات الخارجية وبين احتياجات وإمكانيات وقدرات الأجهزة الإدارية. وهناك عديد من الاتجاهات في الأجهزة الإدارية تبرز الحاجة إلى ضرورة وجود نظام للمعلومات من أهمها الاتجاه إلى زيادة التخصص وتقسيم العمل، وظهور أساليب جديدة في اتخاذ القرارات، والاتجاه نحو اللامركزية في الإدارة، والتوظيف المؤقت للاستفادة من مهارات معينة ولأداء مهام محددة، وبروز ظاهرة العولمة والتحول نحو اقتصاد الخدمات.

أهمية نظم المعلومات للأجهزة الإدارية:

تستخدم نظم المعلومات جميع أنواع التكنولوجيا لتشغيل ومعالجة وتخزين ونقل المعلومات في شكل الكتروني وهو ما يعرف بتكنولوجيا المعلومات التي تشمل الحاسبات الآلية ووسائل الاتصال وشبكات الربط وأجهزة الفاكس وغيرها من المعدات. ويقوم نظام المعلومات بتشغيل البيانات وتقديمها للمستخدمين . ربما يكون فردا أو مجموعة من الأفراد . الذين يقومون بتشغيل مخرجات نظام المعلومات بأنفسهم نتيجة توفر الحاسبات الآلية. وربما تكون مخرجات العديد من النظم مستخدمة بشكل روتيني لأغراض الرقابة على أداء الجهاز الإداري نفسه أو لتبسيط تشغيل

أوامر المستخدمين.

وتعتبر القرارات الخاصة بالتكنولوجيا المستخدمة في الجهاز الإداري العنصر الحاكم في نجاح ذلك الجهاز، فعلى سبيل المثال في الولايات المتحدة الأمريكية ٥٠% من رأس المال المستثمر في الأجهزة الإدارية يتعلق بالمعلومات، كما أن هناك حوالي ٦٣ حاسب آلي لكل ١٠٠ عامل، بينما تقدر بعض المصادر أن واحد من كل ثلاثة من العاملين يستخدم الحاسب الآلي. كما تبلغ نسبة المديرين الذين يستخدمون الحاسب الآلي في أعمالهم حوالي ٨٨%. وبلغ حجم إنفاق الشركات الأمريكية على تكنولوجيا المعلومات في عام ١٩٩٦م ٥٠٠ مليون دولار، بينما بلغ إجمالي الأموال المنفقة في العالم حوالي واحد تريليون دولار.

ويركز المقال على امن المعلومات مع تطور العلم والتكنولوجيا ووسائل تخزين االمعلومات وتبادلها بطرق مختلفه أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح النظر إلى امن تلك البيانات والمعلومات بشكل مهم للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الادوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات وان امن المعلومات هو أمر قديم ولكن بدا استخدامه بشكل فعلي منذ تطور التكنولوجيا .

(/http://ar.wikipedia.org/wiki)

كما ان في المقال فوائد نستطيع تفعيلها في الإدارة التربوية أهمها :

١- التأكيد على دور قاعدة البيانات في المنظمات مما يسهم في تطوير العمل الجامعي .

٢- التأكيد على أهمية تصنيف المعلومات وعلاقاتها بالحماية والخصوصية .

٣- تنوع تعاريف نظم المعلومات الإدارية يعني وجود مرونة في المحتوى والقابلية للتجديد والاضافة .

٤- سياسة المعلومات الإدارية تضمن للمنظمة التعليمية السرية التامة وحماية مصالحها.

٥- يمكن تفعيل وظائف نظم المعلومات بشكل متطور من خلال :

عملية عمل التحليل-تصميم النظام-البحث التقني والتحليل-تطوير تطبيقات جديدة

تكامل الأنظمة-إدارة قاعدةِ البيانات لقواعدِ البيانات المتعدّدةِ-برمجة الأنظمة

دعم وصيانة الأنظمة القائمة- إدارة المشاريع

٦- تصنيف المعلومات الادارية يسهم في توزيع المهام بشكل عادل على الموظفات .

٧- من المعلومات التي تتسم في التعليم كتقييم اداء الموظفات.

٨- والمعلومات الحساسة كمشكلات الطالبات النفسية والمالية .

٩- أما المعلومات الغير مقيدة كالأنشطة المدرسية والحفلات .

١٠- كما يمكن تفعيل المهام أساسية في نظم المعلومات الإدارية كما يلي :

-عدم السماح لغير المستخدمين الدخول على بيانات الطالبات او المعلمات .

-تغيير كلمة السر كل ٩٠ يوم حتى لو لم يجبر النظام لذلك والإبلاغ عن أي اختراق أمني

١١- تعيين مشرفات خبيرا في الحاسب لحماية موقع المدرسة .

١٢- تعيين مشرفات ومطورات للمواقع الالكترونية متفرغات لذلك ولخدمة الموقع التعليمي والزوار.

Administrative Information Systems

Administrative Information Policy

Administrative information is any data related to the business of being an Institution of Higher Learning. Jackson State recognizes administrative information to be a University resource which requires proper management in order to permit effective planning and decision making and to conduct business in a timely and effective manner.

Administrative information does not include library holdings or research or instructional notes unless they contain information which relates to a business function. Such functions include (but are not limited to) financial, personnel, student, alumni, communication, and physical resources data. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which it resides.

Jackson State retains ownership of all administrative information created or modified by its employees as part of their job functions.

Administrative Information Systems

Functions of the Administrative Information Systems Group

The Administrative Information Systems group provides information technology solutions and services which enhance the academic mission and business process of The College of Agriculture and Life Sciences. The broad range of functions include:

- Business Process Analysis
- System Design
- Technical Research and Analysis
- Development of New Applications
- Integration of Systems
- Database Administration for multiple databases
- System Programming
- Support and Maintenance of Existing Systems
- Project Management

These functions are utilized to assist campus faculty and staff in meeting their teaching, research and extension needs through provision of leading technology decision support systems and sophisticated financial and administrative information reporting systems.

Data Management Resource Team (DMRT)

The Data Management and Resource Team is responsible for creation of efficient data management systems for use in historical and current financial and management report development, deployment and maintenance that are in alignment with institutional needs and goals.

Special Projects

Special Projects group provides technical guidance on the most complex projects, provide input and guidance on technical directions, and formulate infrastructures and architectures in support of CALS business.

Classification of Data

For security purposes, administrative information can be categorized into three levels of protection:

Confidential
information that requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of the University to accomplish its mission as well as records about individuals requiring protection under the Family Educational Rights and Privacy Act of 1974 (FERPA) and data not releasable under the Freedom of Information Act.

Sensitive
information that requires some level of protection because its unauthorized disclosure, alteration, or destruction will cause perceivable damage to the University. It is assumed that all administrative output from the central computing facility is classified as sensitive unless otherwise indicated.

Unrestricted
information that can be made generally available both within and beyond the University.

Data Security Policy

Administrative information is one of Jackson State's most valuable resources and requires responsible use by members of the University community. Jackson State employees are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of employment. Employees are expected to act in a manner that will ensure the information which they are authorized to access is protected from unauthorized access, unauthorized use, invalid changes, or destruction.
Access to administrative systems is granted to a particular individual based on the need to use specific data, as defined by job duties, and subject to appropriate approval. As such, this access cannot be shared, transferred or delegated. Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination.

The provisions of the Information and Data Security Manual detail the responsibilities of Jackson State employees in maintaining the security of administrative information. These individuals are also subject to the policies contained in Using Computing Resources at Jackson State University as well as guidelines specific to the information which they access. The sections that follow define responsibilities, establish authorization, and provide guidelines to assist people in the handling of this resource - information.

Employees

Definition:

The term "employee" is used in this manual in its most general sense to incorporate not only people paid by the University for their work but also those who perform service for Jackson State and are granted access to administrative information. The term as used here does not, in and of itself, confer any special status or relationship with the University and is not intended to confer employee status. In addition to regular staff and faculty, the term employee includes temporary staff, student employees, consultants, volunteers, and adjunct, emeritus, and visiting faculty.

Responsibilities:

Employees are responsible for the security of administrative data. While these guidelines provide examples of appropriate care, they are not intended to be exhaustive of all activities that ensure this security. Staff are expected to evaluate their actions with respect to the protection of administrative data and to act in a manner which is in the best interest of the University.
Requests for access to electronic administrative information must be made using the appropriate forms in the Administrative Information Systems Forms Package available from the department computer liaisons (Administrative Information Coordinators or Department Computing Coordinators). Included on each form must be sufficient information to determine why an employee needs the requested access and the signatures of required authorized administrators.
The following outlines the responsibilities of an employee:

- **Refrain from accessing and using information in unauthorized ways**
  Employees who attempt unauthorized access to administrative computer access IDs are subject to disciplinary measures. Employees must not access microcomputers which have not been provided to them for their work without the express permission of their supervisor. They are also responsible for refraining from perusing administrative data not specifically provided to them for their work (even when it is left in an unprotected area) and from entering areas where administrative information is stored unless they are authorized to do so.
- **Follow procedures for storage of data**
  Employees are required to follow departmental procedures which specify where administrative information is to be stored and the precautions associated with its storage. Such precautions include:

- **Securing copies of administrative information, such as microfiche and printouts, in file cabinets or desks.**
- **Storing non-reproducible information in areas designed to safeguard it from unauthorized viewing and damage from natural cause.**
- **Storing floppy disks in a locked file cabinet or desk. Disks with sensitive information must be locked in a cabinet with a non-standard key lock.**
- **Regularly backing up locally maintained administrative information stored on disk to ensure that information is not lost in the event of disk failure.**
- **Placing confidential data stored on a hard disk in a segment that is protected by an approved security program requiring an access password.**

- **Follow procedures for dissemination of data**
  Distribution of administrative information must be accomplished through approved procedures.
  - **Safeguarding the dissemination of information by phone, fax or printed materials to those approved to receive the data by following departmental procedures that conform to the policies established by the Data Responsible Custodian for that data.**
  - **Transferring, via network, computerized copies of administrative data through approved University procedures. Copies transferred by floppy disk follow procedures for non-computerized dissemination.**
- **Follow procedures for disposal of data**
  Employees must adhere to departmental procedures specifying how administrative information is to be disposed of when it is no longer needed for business purposes.
  - **Shredding or burning of paper or microfiche copies to ensure the security of the information.**
  - **Observing retention guidelines in selecting documents to be destroyed.**
  - **Erasing recording tapes (from Dictaphones or recorders); not just writing over them.**
  - **Properly discarding computer disks (hard disks and floppy) containing administrative information. Mac disks must be re-initialized. Other PC disks require a more sophisticated utility to remove access to the data.**
- **Protect data from unauthorized access**
  Keys and access cards that permit entry into storage facilities where confidential data is stored must not be loaned or left where others could use them to access the secure areas. Passwords are the key to accessing on-line administrative information.
  - ***Never share passwords,* even with a supervisor.**
  - **Select passwords which are not obvious choices. Passwords other than family member names, nicknames, and words found in a dictionary make it more difficult for someone to discover a password (e.g. LQREFW or JK224L).**
  - **Never tape passwords to a wall, under a keyboard or in other easily discoverable areas.**
  - **Change passwords every 90 days even if a system does not force it.**

In order to protect centrally maintained administrative information from unauthorized viewing, workstations must be logged off to a point that requires a new log-on whenever employees leave their work area, except for specially designated areas. All access IDs must be logged off whenever an employee leaves for the day. Employees must also follow policies regarding the physical security of computer equipment.
Screens must be oriented to prevent unauthorized people from reading sensitive information. The location of the screen must face away from any traffic areas.

- **Report any breach of security**
  When there is an actual or suspected breach of security that might compromise administrative information, the incident must be reported immediately for investigation to the supervisor, the Information Security Officer, or the University Auditor

---

Supervisors

Definition

The term "supervisor" is used in this manual in its most general sense to incorporate not only people whose job function is defined to include supervision of staff but also to apply to people who informally direct the work of others. Such titles as supervisor, manager, director, chairperson, department head, dean and vice president are used to formally denote supervisors; however, many other positions are also supervisory.

Responsibilities:

It is the responsibility of supervisors to maintain a high level of security in the work place. Supervisors have a responsibility to inform their staff of the proper manner of handling administrative information, to evaluate the effectiveness of these procedures, and recommend changes to improve this security. In addition to the security responsibilities applicable to all employees, supervisors have responsibilities regarding data security as outlined below:

- **Review access of their staff**
  Staff with a need to access administrative information as determined by the chairperson/department head are to be issued keys, access cards, and/or combinations to areas where administrative information is maintained within the guidelines for access established by the chairperson/department head. Special locks which provide a higher level of security than those provided by furniture manufacturers can be obtained from Plant Operations and must be used to protect sensitive administrative information. Supervisors must review the physical access of their staff periodically (as defined by departmental procedures) at least annually since staff can assume different responsibilities within a department over time.
  Supervisors must review all requests by their staff for access to computerized administrative information. The requests must fall within

the departmental guidelines of appropriate access to be approved. Supervisors must review the access of each staff member periodically. Supervisors are also responsible for providing copies of this policy and manual to consultants, temporary staff and other special employees and assisting them as needed to understand the policy.

- **Ensure that employees comply with security policies and procedures**
  Supervisors should recognize and encourage staff who are particularly conscientious in the proper handling of administrative information. Supervisors must counsel staff who violate security procedures as outlined in the Employee section of this manual and are responsible for managing improvements in staff behavior. If violations continue, the problem must be resolved.
- **Monitor use to identify problems**
  Supervisors must ensure that upon the conclusion of the work day staff have properly secured administrative information and must periodically observe the staff work areas for persons attempting to gain access to documents left unattended. Supervisors are also responsible for noting employees' behavior that constitutes "browsing" through data beyond the needs of their positions.
  Reports of usage and other access information must be reviewed by supervisors to ensure that staff are properly using their access. Supervisors must report problems to the chairperson/department head and assist appropriate University personnel in the resolution of the problem.
- **Remove access when staff leaves the department**
  Supervisors must ensure that staff who terminate their employment with the department return their physical access keys and cards on their last day of work in the department. Staff who are dismissed from the University must return their keys/cards at the time they are notified of their dismissal. If this does not occur, access cards must be immediately canceled and areas controlled by the outstanding keys must be reprogrammed.
  When an employee separates from the department voluntarily or by transferring, IT must be notified to close his/her access at the end of the employee's last day in the department. However, when disciplinary measures are involved, the supervisor must report the dismissal to the Information Security Officer prior to meeting with the employee in order that the computer access can be canceled during the meeting.

Chairperson/Department Heads

Definition

The term "chairperson/department head" is used to denote the director of an administrative, academic or research unit within the University. This person has full fiscal responsibility for the department including preparing budgets and monitoring spending. A chairperson/department head reports directly to a senior administrator.

Responsibilities:

The chairperson/department head is responsible for establishing an environment of security awareness for the data handled by the department. (S)he sets procedures related to the security of the data and supports these procedures by the distribution of funds. Chairpersons/department heads must review office procedures at least on an annual basis and make updates to respond to changes in technology and policies. Annual budgets should anticipate the need for funding of resources to protect administrative information located in the department. In addition to the security responsibilities applicable to all employees and supervisors, chairpersons/department heads have the following responsibilities regarding data security:

- **Translate policies into office procedures**
  The Data Security and Administrative Information policies contained in this manual form the basis upon which office procedures are to be developed to protect administrative information. Procedures should ensure that access is provided based on information required to perform the assigned work. Practices that reflect handling of specific types or classifications of data should be included in office practices. Office procedures must address the following situations:
  - **The transfer of non-electronic forms of administrative information must maintain a level of security which ensures that only people authorized to handle the data have access to it. Procedures must include specific measures to be taken to protect confidential information and to track the flow of data through the department and between sections within department (for instance, by means of logs).**
  - **Virus checkers must be installed on all microcomputers that maintain administrative information to protect the data from destruction or distortion.**
  - **Chairpersons/Department Heads must ensure that computer repairs are undertaken in a manner that protects the confidentiality of the data stored in the system. Whenever possible, the Jackson State University Computer Repair facilities must be used. If the equipment requires the use of outside repair facilities, the purchase contract for the work must include non-disclosure statements regarding information stored on the hard disk and within the system.**
  - **Networks within the department must be properly secured to prevent unauthorized access.**
- **Provide resources to implement procedures**
  - **When non-electronic administrative information is no longer needed in the department, mechanisms that will ensure its proper disposal must be available. Confidential information must be shredded within the department or transported securely for shredding or burning at a proper facility.**
  - **Storage (temporary or permanent) of non-electronic forms of administrative information must safeguard against the information's unauthorized viewing as well as loss due to accidents or acts of nature. The Chairperson/ Department Head must provide for adequate storage facilities and locking devices to ensure this protection.**

- **Sensitive or critical administrative information maintained locally on microcomputers must be kept within an electronic partition that requires a password to gain access. The chairperson/department head is responsible for ensuring that either funds are available for the purchase of software with this locking capability or that the information is not maintained on the hard disk.**

- **Determine sensitivity of non-centralized data originating in the department**
  The chairperson/department head must define the level of confidentiality of data originated within that department based on existing state and federal laws and the potential impact of that information's loss on the business functioning of the University. Using the "need to know" guideline, (s)he is responsible for determining the dissemination of the data and for educating its users in the proper care of administrative information. Data which the chairperson/department head classifies as "unrestricted" must fall within the guidelines for release set by the office of University Relations before it is disseminated beyond Jackson State.

Data Responsible Custodians

Definition

The Data Responsible Custodians constitute a body of knowledgeable users who function as trustees of the University's administrative information. For each centrally maintained administrative application, a director or manager of a functional unit (department) is assigned the authority for making decisions related to the development, maintenance, operation and access of the application and the data associated with that business function.

The Data Responsible Custodians are responsible for establishing guidelines for the management and protection of this data and for making recommendations to improve the availability of this University resource. Each Data Responsible Custodian is responsible for a subset of administrative information which (s)he protects in the following ways:

- **Maintain detailed knowledge of the data within their trust**
  The Data Responsible Custodian is expected to be the person most familiar with the business functions to which the data applies, the structure and functioning of the database management system(s) in which the data resides, and the methods available for accessing the data. The Data Responsible Custodian must be thoroughly familiar with the data itself, including valid values and data transformations, and also be able to assist with an analysis of the impact of field changes and with applying data retention laws and practices.
- **Manage activity related to the business information**
  The Data Responsible Custodian evaluates, approves, and prioritizes requests for changes to the business system(s) for which (s)he is responsible. In addition, (s)he will communicate to the Administrative

Computing Committee any major changes in business practices which would seriously impact the system's ability to continue to provide necessary service.
In conjunction with his/her counterparts and staff of Information Technology, the Data Responsible Custodians develop recommendations for the Administrative Computing Committee regarding policies and procedures to manage business information. This group also coordinates planning activity related to the business needs of the various functional areas.
Data Responsible Custodians, with the recommendations of Computing and Information staff, assist the Administrative Computing Committee with the development of long range administrative computing goals and with the translation of these goals into schedules for application replacement or major overhaul along with recommendations for specialized hardware to support these changes.

- **Develop guidelines for requesting access**
  Using their familiarity with the data elements, the Data Responsible Custodians translate job responsibilities into access capabilities to assist supervisors in developing guidelines for employees' access to data. These guidelines must reflect any state or federal laws governing the dissemination of the information in their trust.
- **Review requests for access to administrative information**
  All requests for access to the data entrusted to a Data Responsible Custodian, both on-line and through batch, will be reviewed and (1) approved, (2) modified or (3) denied in keeping with the established guidelines and general security practices. Data Responsible Custodians (or their delegates) will assign access based on the specific data which is required for an employee to do his/her job.
- **Define the sensitivity of the data**
  Each Data Responsible Custodian is responsible for identifying data elements or combinations of data elements within his/her trust that must be handled with a high level of protection and designated as "confidential" either because of state or federal laws governing the data or because it is determined by the DRA that it is in the University's best interest to afford the information special protection. All other data elements will be assumed to be classified as "sensitive" unless specifically designated as "public" by the Data Responsible Custodian. This classification will be used to define the proper handling of information in an employee's use.
- **Develop guidelines for proper handling of administrative information**
  The Data Responsible Custodians will develop and maintain guidelines regarding the creation, viewing, modification, storage, transmittal and disposal of administrative information based on the level of sensitivity of the data. Where state or federal laws dictate the special handling of certain data, the Data Responsible Custodian entrusted with the information will ensure that the exceptions are included in the guidelines.
- **Review usage information**
  For those systems for which information on system usage is available, the Data Responsible Custodian is responsible for reviewing usage reports promptly to detect potential misuse of access, identify employees who may need additional training in the use of the data, extract usage trends, and observe any abnormalities that may indicate data or access problems. The

Data Responsible Custodian works with the Information Security Officer to clarify and correct any problems noted.

- **Assist in developing standardized security practices**
  The Data Responsible Custodians assist the Information Security Officer in developing consistent security practices throughout the University and educating employees in these practices. These practices will be documented in the security manual and reviewed periodically by the Data Responsible Custodians to ensure that they are appropriate in light of changes in the technology and direction of the University.
- **Assist with business resumption planning**
  The Data Responsible Custodians, in conjunction with Information Technology staff, are responsible for developing and maintaining plans which would allow the business functions of the University to continue in the event of an interruption of service. These plans include not only the ability to recover centrally maintained software applications but also business functions that are resident within the business unit itself.

Administrative Computing Committee

Definition

The term "Administrative Computing Committee"(ADCC) refers to a group of senior officers who determine the direction of and, ultimately, the policies associated with administrative computing. These officers include the President, the Vice President for Information Technology and the Vice President for Finance or their designated representatives.

Responsibilities:

The Administrative Computing Committee has responsibility for ensuring the protection of Jackson State's administrative information, establishing policy and philosophies for information and data security, and assigning responsibilities to various University employees to assist the Committee in these matters. Their responsibilities with respect to information and security are:

- **Review and evaluate plans for administrative information systems**
  The Administrative Computing Committee has the responsibility for the execution of all policies related to the management of business information. The ADCC, with the assistance of Data Responsible Custodians and Information Technology staff, will develop long range plans for administrative computing systems and set priorities to reflect the goals of the University. The ADCC will review, evaluate, and approve specific maintenance or replacement plans for administrative systems in keeping with the computing needs of the University and the availability of fiscal resources. It is also the responsibility of the ADCC to review and evaluate the progress of these plans.
- **Review and approve policies**
  The Administrative Computing Committee is responsible for reviewing and approving the Information Policy and the Security Policy to ensure

that these policies complement and adhere to the business philosophies of Jackson State. Any modifications to these policies must also be reviewed and approved by this committee.

- **Review security controls**
  The Administrative Computing Committee reviews philosophies and general plans which control security and monitor use. This group oversees the protection of administrative information while maintaining the individual rights of employees, and sets priorities for security plans in relation to current and anticipated resources.
- **Provide the means to implement the policies**
  In order for the policies to be effective, they need to be integrated into the work environment. The Administrative Computing Committee, through various procedures, facilitates the implementation of these policies. The committee is responsible for identifying sources of funding to implement policies and procedures as necessary.
- **Enforce policies**
  In the event of a serious security breach, members of the Administrative Computing Committee will review reports and evidence (including the convening of a hearing if necessary) to determine culpability, define the exposure of the University from the breach, consider steps to decrease the exposure of the University from the breach, minimize the potential for a similar breach to occur in the future, and if appropriate, determine what disciplinary action will be taken toward the individual(s) involved.
- **Clarify and interpret the policies**
  Questions related to the scope or implementation of the policies may be referred to the Administrative Computing Committee for resolution. Although the Data Responsible Custodians and the Information Security Officer are the primary contacts for these types of questions, members of the Administrative Computing Committee may be asked to review procedures as they relate to the business philosophies of the institution.
- **Ensure that policies remains current**
  As technologies and practices evolve at Jackson State, the Administrative Computing Committee is responsible for ensuring that policies adequately protect the University. When policies need to be revised to meet changes, the Administrative Computing Committee will assign this responsibility to appropriate University staff.

Internal Auditors

Definition

"Internal auditor" is used in this manual to refer to the University Auditor and other members of the Internal Audit staff. It is not applicable to auditors who are not employees of Jackson State. The internal auditors provide an objective and independent perspective to the University on the security of its information resources.

Responsibilities:

In accordance with the University Auditor's charter, Jackson State's internal auditors are authorized inquiry-only access to all administrative information and systems, and are responsible for assisting supervisors in the effective discharge of their duties. In addition to being subject to information security policies applicable to other Jackson State employees, Jackson State's professionally certified internal auditors must adhere to auditing standards and ethics codes established by applicable certifying groups. In exercising their duties relating to information security, internal auditors:

- **Evaluate compliance with information security policy and procedures within University departments during operational and administrative audits.**
- **Evaluate the effectiveness of security procedures and other internal controls to limit access to administrative information appropriately, and identify and recommend improvements for areas of vulnerability.**
- **Review audit trails provided by the application security systems to assess if activity is adequately documented to allow for errors or improprieties to be identified, traced to their source, and corrected.**
- **Assist management in the investigation of suspected incidents of security breach or improper activity.**
- **Provide advice on internal controls relevant to new systems being developed or being considered for purchase.**

Computing Services and IT Staff

Responsibilities:

Computing Services and Information Technology (IT) staffs have the expertise and the responsibility to protect administrative information residing on the University's mainframe, network, and local servers and must use this expertise in a responsible manner to ensure the integrity of the data and the availability of the information. Because of their greater opportunity to access administrative information, IT staff and Computing Services staff have the following additional responsibilities.

- **Adhere to the department's non-disclosure agreement**
  Every employee in IT and Computing Services must read and sign a non-disclosure statement as a condition of employment. Staff must follow the restrictions placed upon them by the agreement in addition to the policy on information security.
- **Maintain data and programs within established standards**
  All data set names must conform to the naming conventions adopted by IT or Computing Services. Staff will not rename or create a data set with a name contrary to the standards to circumvent the security protecting these resources.
  Programs will be developed or modified following standards established

by the department. Also, standardized mechanisms of documenting changes will be observed.

- **Provide security for computer systems**
  Computing staff are responsible for following departmental procedures in regard to the physical protection of equipment in Jackson State's computer system. This includes (but is not limited to) mainframes, microcomputers, workstations, servers, printers, external storage devices, modems and any other hardware components as well as the physical network that joins these machines. Where physical access is restricted by security devices, staff will not share their entry "key" or circumvent the security system. Visitors to a secure area where computer equipment is housed must be escorted by a departmental staff person who assumes, along with the visitor, responsibility for the physical and logical integrity of the machines during that period.
  As part of the safeguard of computer systems, regular backups will be produced to permit reconstruction of the system in the event of file or equipment damage. These backups will be stored at a different location from the systems equipment and off campus for critical business systems.
  System software will be applied/modified following the procedures defined by the vendor for the equipment on which it resides. Any "bugs" will be corrected as quickly as possible by the systems staff and, if appropriate, users will be advised of the potential inaccuracies which the error could cause.
  Administrative databases will be managed following acceptable standards including the review of available space to ensure that sufficient area exists, the inclusion of data value checks in data entry programs, the activation of usage reporting mechanisms, and the regular production and review of usage reports.
- **Assist with the development of long range plans**
  Information Technology staff will assist the Data Responsible Custodians in the development of recommendations to the Administrative Computing Committee of long range administrative computing goals. They will also assist with the translation of these goals into schedules for application replacement or major overhaul as well as recommendations for specialized hardware to support these changes.
- **Training and consulting with departmental computing liaisons**
  Departmental Network Administrators, Departmental Computing Coordinators, Administrative Information Coordinators and Data Responsible Custodians serve as liaisons between their departments and centralized computing services. IT and Computing Services provide special training to these staff to maintain their level of competence as technologies change. In addition, IT and Computing Services staff support computing liaisons' efforts within their departments by responding to their questions and problems.
- **Assist with development of business resumption plans**
  Information Technology staff, in conjunction with Data Responsible Custodians, will develop and maintain plans which would restore services to centrally managed hardware and application software systems in the event of an interruption of service. The plan will include information to assist in determining the sequence for restoring critical business applications.

Information Security Officer

Responsibilities

The Information Security Officer is responsible for establishing and monitoring procedures to ensure that Jackson State's administrative information is secure from unauthorized access, protected from inaccurate modification, and available to authorized users in a timely manner to enable them to perform their work. Included in these responsibilities is the necessity to be technically fluent with the various security systems used to protect data and to compensate, by the use of procedures, for any shortcomings of these systems. Specifically the responsibilities include the following:

- **Develop and maintain effective security procedures**
  The Information Security Officer is responsible for developing, in conjunction with the Data Responsible Custodians, procedures to implement the data security policies of the University. An important part of this task is to review all access reports and logs. The Information Security Officer will periodically make a system-wide review of access provided to users to ensure that the access is consistent with established guidelines for the system and that the guidelines provide the necessary access.
  As new or revised systems are introduced, the Information Security Officer works with the appropriate Data Responsible Custodian(s) to review and advise in the development of procedures to protect the information and to document the access. These procedures must include mechanisms for:
  - **compensating for the inadequacies of the security system**
  - **reporting on the activity of the system**
  - **providing users access to the data**
  - **disseminating information to users on the appropriate handling of the data.**
  - **destroying non-electronic versions of the information**

For existing systems, the Information Security Officer, in conjunction with the Data Responsible Custodian(s) and the appropriate development team, reviews current procedures to ascertain that they provide an adequate level of protection and, as needed, makes recommendations to bring them into compliance with accepted standards of security.
If a breach occurs in a security system, the Information Security Officer will review the guidelines and procedures of the system and, if necessary, recommend any changes to better protect the University's data.
For systems that are delivered without a complete set mechanisms for activity reporting, the Information Security Officer will work with the appropriate development team to define the data to be retained and the manner of reporting.

- **Test and document administrative security systems**
  Using standard testing procedures, the Information Security Officer is responsible for determining the scope of security provided by the various subsystems used at Jackson State to protect administrative information

and to document these systems. Included in this documentation are any restrictions, anomalies, shortcomings, and exposures.

- **Consult on internal security issues**
  The Information Security Officer is responsible for advising the Data Responsible Custodians, internal auditors, and senior management in regard to the technical functioning of the security subsystems of administrative systems.
  (S)he also consults with developers, systems support staff and users to ensure that adequate security features are included in new or modified administrative system software.
- **Prepare and maintain general security policies and guidelines**
  The Information Security Officer is responsible for producing and maintaining the University's data security policies subject to review and approval by the Data Responsible Custodians, the Administrative Computing Committee, and senior management at the University. Supporting documentation for these policies is developed by the Information Security Officer in conjunction with the Data Responsible Custodians and, as technologies and policies evolve, their contents are updated by the Information Security Officer.
  The Information Security Officer assists the Data Responsible Custodians in developing and maintaining guidelines for the proper handling and use of the administrative information in their domain. (S)he assists in disseminating these guidelines to the departments that use the data. The Information Security Officer can also assist Chairpersons/Department Heads in developing departmental procedures to implement the general guidelines established by the Data Responsible Custodians.
- **Provide assistance with security training**
  The Information Security Officer is responsible for providing information for general security awareness training as well as specific education on the University's security policies and the security manual. (S)he may also assist the chairperson/department head in preparing training materials for his/her staff on departmental security procedures. It is the responsibility of the Information Security Officer to assist in interpreting the policies with regard to specific situations that arise and to assist in educating users to be able to make decisions consistent with these policies.
- **Review the data access repository**
  In order to determine the total access each user has to administrative data, the Information Security Officer is responsible for periodically reviewing the repository of information containing the privileges for each user across administrative systems. This review must ensure that users have the access they need to perform their work and that their overall access is in compliance with general guidelines of security.

Access ID Managers

Responsibilities

Access ID managers are Jackson State employees whose duties include the creation, deletion, or modification of access IDs or the maintenance of tables of

access IDs which control the ability to view or update administrative information. Because of the scope of this capability, additional responsibilities are assigned to access ID managers as follows:

- **Maintain complete documentation for all changes**
  Before any access ID or table is modified, written documentation must be completed that includes the original signatures of the access ID owner, his/her supervisor, and the appropriate Data Responsible Custodian(s). In special circumstances, electronic mail is permitted in lieu of a signed form; these exceptions will be reviewed and documented prior to implementation. Access ID managers are responsible for maintaining all forms of change documentation for audit purposes.
  Especially in cases where the Data Responsible Custodian also functions as the access ID manager, any changes to access IDs must be reviewed by the ISO prior to implementation.
- **Implement access defined by the Data Responsible Custodians**
  Access ID managers must accurately transfer the access defined by the Data Responsible Custodians into the access ID definition. If access definition is vague or inconsistent, the access ID manager will return the request to the appropriate Data Responsible Custodian for clarification.
- **Suspend access when employees terminate or transfer**
  Using information provided by the Human Resources office, access ID managers will delete IDs of employees who have separated from the University and will lock or delete the IDs of employees who transfer to other departments within Jackson State. When special arrangements have been made for an employee to have access beyond his/her last official day in the department, access ID managers will set an expiration date on the access ID (if the security permits) or will maintain a "tickler" file to remind them to delete the access ID at the end of the extension period.

System Changes

- **Production System**
  All changes that are proposed for the production environment must be approved by senior level management. Any individual or group who will be affected by these changes must be notified in writing prior to the changes being made. Changes must be made in the test environment and verified before they are placed into production. Application system changes must be approved by that system's custodian and a member of the computer center's staff before they are made. Once approved, these changes must be installed in the test environment and thoroughly tested by the computer center staff and the end user community before being placed into production.

- **Data Communications**
  Proposed changes to the university's network configuration must be approved by the computer center's management before being made. All changes must be first made in the test environment initially, where the changes must be tested and verified as being correct, by the person requesting the change, and members of the IT staff. New VTAM definitions must be created for the modification, and changes must not be made to the production VTAMLST member. After new definitions are tested and verified they may be placed into production. At this point the old definitions must be archived.

Appendix A - Definition of Terms

Access ID Manager:

Access ID Manager is an employee whose duties include the creation, deletion, or modification of access IDs or the maintenance of tables of access IDs which control access to administrative information.

Administrative Computing Committee

The term "Administrative Computing Committee" refers to a group of senior officers who determine the direction of and the policies associated with administrative computing. These officers include the President, the Vice President for Information Technology and the Vice President for Finance or their designated representatives.

Administrative Information Coordinator:

The Administrative Information Coordinator is responsible for the timely and accurate processing of information needed to run the University. The Coordinator represents his/her department in matters related to the administrative production environment by meeting regularly throughout the year with administrative support staff in IT.

Chairperson/Department Head:

The term "chairperson/department head" denotes the director of an administrative, academic or research unit within the University. This person has full fiscal responsibility for the department including the preparation of a budget and monitoring of spending. A chairperson/department head reports directly to a senior administrator.

Confidential data:

information that requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of the University to accomplish its mission as well as records about individuals requiring protection under the Family Educational Rights and Privacy Act of 1974 (FERPA) and data not releasable under the Freedom of Information Act.

Data Responsible Custodian:

The Data Responsible Custodians constitute a body of knowledgeable users who function as trustees of the University's administrative information. For each centrally maintained administrative application, a director or manager of a functional unit (department) is assigned the authority for making decisions related to the development, maintenance,

operation and access of the application and the data associated with that business function.

Department Computing Coordinator:

The Department Computing Coordinator is a faculty, staff or graduate student assigned by a department to provide individualized computer support in the department environment.

Departmental Network Administrator:

The Departmental Network Administrator is responsible for supporting the networking environment in his/her department. Responsibilities include installing applications on a departmental server and providing first-level support and trouble-shooting on network related questions.

Employee:

The term "employee" is used for the purpose of this statement to incorporate not only people paid by the University for their work but also those who perform some service for Jackson State and are granted access to administrative information. The term as used here does not, in and of itself, confer any special status or relationship with the University and is not intended to confer employee status. In addition to regular staff and faculty, the term employee includes temporary staff, student employees, consultants, and adjunct, emeritus, and visiting faculty.

Internal Auditor:

The term "internal auditor" is used to refer to the University Auditor and other members of the Internal Audit professional staff.

Information Security Officer:

The Information Security Officer is the person responsible for establishing and monitoring procedures to ensure that Jackson State's administrative information is secure from unauthorized access, protected from inaccurate modification, and available to authorized users in a timely manner to enable them to perform their work.

Public data:

information that can be made generally available both within and beyond the University.

Security:

Information is secure only when its integrity can be maintained, its availability ensured, its confidentiality preserved, and its access controlled.

Sensitive data:

information that requires some level of protection because its unauthorized disclosure, alteration, or destruction will cause perceivable damage to the University.

Supervisor:

The term "supervisor" not only incorporates people whose job function is defined to include supervision of staff but also applies to people who informally direct the work of others.

Appendix B - Alternate Classifications of Data

The classifications schemes below provide alternative views to the classifications used for data security. The three dimensions - function, scope and purpose - catagorize data along a continua in a form that will encourage its scalableness in a standard, consistent and accurate way. The goal of these classification schemes is to ensure the independence of data from organizational structure and software application.

Functional Areas:

Functional area is defined as the primary University purpose served by the data. As such, it does not necessarily follow organizational lines of authority. Due to extensive integration across functional units, functional classification may be discretionary. Therefore a functional unit may be given authority for data that is shared by many other organizational units. The functional area classifications are:

Student Data

> **Student data supports all phases of a student's relationship with the University from application through alumni status, except as noted elsewhere. This includes (but is not restricted to) demographic data, academic records, disciplinary and medical records, course information, admissions data, financial and non-financial student data, and development information.**

Financial Data

> **Financial data supports the management of fiscal resources of the University and includes accounting, budgeting, accounts payable, accounts receivable, loans, investments, capital assets, and payroll information.**

Human Resources Data

> **Human resource data supports the management of employee resources of the University, including all types of information related to employees as defined previously. This data includes employee demographics, retirement and EEO data, vita, employee evaluations, promotion and disciplinary data.**

Business Affairs Data

> **Business affairs data supports the auxiliary and related enterprises of the University such as retail sales, central supplies, graphic services, and telecommunications.**

Facilities Data

> **Facilities data support the facilities and services resource of the University including space planning data; construction, maintenance and operational data, reservations and physical descriptive information.**

Material Data

> **Material data provides information for all aspects of equipment, furniture, and expendable materials resources (e.g. inventory and purchasing information).**

External Relations Data

> **External relations data supports activities which interface between the University and the rest of the community. This includes ticketing, publications, and public information.**

Scope:

The scope of data is defined as the breadth of its impact on the University's mission or the range of its reach within the University. The following categories define the scope of data:

University wide

This data provides support to and meets the needs of essentially all units of the University. Examples of this type of data include many of the elements supporting financial management, payroll, personnel management, and capital equipment inventory.

Inter-departmental

This data provides support to and meets the needs of more than one University unit. This information, while less important for the operation of the entire University, are still critical to a broad cross-section of the school. Such data elements as those supporting admittance of students, student records, financial aid, and loans are examples of this type of data.

Intra-departmental

This data provides support for a single functional unit or department or is relatively narrow in terms of the impact on the University. Despite its limited range, it is considered essential to the business function it supports.

Independent

This data is limited to a single user or a few individuals within a department who perform similar tasks.

Purpose:

The purpose of the data is defined as the role played by the data element in serving the University. This classification implies a hierarchy with operational at the lowest level, management at the middle, and strategic at the highest. While described as individual entities, in practice, much data falls across several categories and where that occurs, it has been classified at the higher level.

Operational

This type of data element is the basis of record-at-a time, transaction driven applications. This category refers to the raw, elementary data elements from which synthesis and analysis can occur.

Management

This type of data is the summary and control information often derived from the operational data. It is used to make decisions regarding the University's routine operations and, in general, is predictable and foreseeable.

Strategic

This type of data provides the basis for strategic planning and decision support. Often the complexion and nature of this data is not predictable until the planning process is initiated or a problem formulated. Modeling, data concatenation, and advanced data analysis techniques are used to produce this type of data.

نظم المعلومات الإدارية

سياسة المعلوماتِ الإداريةِ

المعلومات الإدارية هي أي بيانات تتعلق بالأعمال من أن تكون مؤسسة التعليم العالي. ولاية جاكسون عرفت المعلومات الإدارية لتكون مصدر جامعي الأمر الذي يتطلب الإدارة الصحيحة من أجل السماح للتخطيط الفعال واتخاذ القرارات ولإجراء العمل في الوقت المناسب وبأسلوب فعال.

المعلومات الإدارية لا تتضمن مقتنيات المكتبات أو البحوث أو مذكرات تعليمية إلاّ إن كانت تحتوي على المعلومات التي تتعلق بوظيفة العمل. مثل هذه الوظائف تشمل (ولكن ليس محصورة إلى) المالية، وشؤون الموظفين، الطلاب، الخريجين، الاتصالات، وبيانات الموارد الفيزيائية. وهي تشمل البيانات التي حفظت في الإدارات ومستوى المكاتب، بغض النظر عن أجهزةِ الإعلام التي تسكن فيها.

ولاية جاكسون احتفظت بملكية جميع المعلومات الإدارية التي تم إنشاؤها أو تعديلها من قبل موظفيها كجزء من مهام وظائفهم.

نظم المعلومات الإدارية

وظائف مجموعةِ أنظمةِ المعلوماتِ الإداريةِ

مجموعة أنظمة المعلومات الإدارية توفر حلول تكنولوجيا المعلومات والخدمات التي تعزز المهمة الأكاديمية وعملية عمل كلية الزراعة وعلوم الحياة. التشكيلة الواسعة للوظائف تتضمن:

- عملية عمل التحليل
- تصميم النظام
- البحث التقني والتحليل
- تطوير تطبيقات جديدة
- تكامل الأنظمة
- إدارة قاعدةِ البيانات لقواعدِ البيانات المتعدّدةِ
- برمجة الأنظمة
- دعم وصيانة الأنظمة القائمة
- إدارة المشاريع

هذه الوظائف استخدمت لمساعدة أعضاء هيئة التدريس في الحرم الجامعي والموظفين في اجتماع تعليمهم، البحوث وحاجات التمديد من خلال بند قيادة تقنية قرار دعم الأنظمة وتطور مالي والمعلومات الإدارية التي تبلغ عن الأنظمة.

فريق موارد إدارة البيانات (DMRT)

إن إدارة البيانات وفريق الموارد مسؤولين عن إنشاء أنظمة فعالة لإدارة البيانات لاستخدامها في المالية الحالية، وتطوير تقرير إداري، والانتشار والصيانة التي تتوافق مع حاجات المؤسسات والأهداف.

المشاريع الخاصة

مجموعة المشاريع الخاصة تزود التوجيه التقني على المشاريع المعقدة، وتزود المساهمة والتوجيه على الاتجاهات التقنية، ويصوغ البنى التحتية والهندسة المعمارية في دعم عمل سي أي إل إس.

تصنيف البيانات

لأغراض أمنية، المعلومات الإدارية يمكن أن تصنف إلى ثلاثة مستويات من الحماية:

سري أو خصوصي

المعلومات التي تحتاج إلى مستوى عال من الحماية بسبب الخطر ومقدار الخسارة أو الأضرار التي يمكن أن تنجم عن كشف أو تعديل أو تدمير البيانات. وهذا يشمل المعلومات التي ساء استخدامها أو الكشف عنها يمكن أن يؤثر سلبياً على قدرة الجامعة على إنجاز مهمتها بالإضافة إلى السجلات حول الأفراد الذين يتطلبون الحماية تحت الحقوق التربوية العائلية وقانون سري من ١٩٧٤ وبيانات غير مبعثه تحت قانون حرية المعلومات.

حساس

المعلومات التي تحتاج إلى بعض من مستويات الحماية لأن الكشف عنها غير مرخص، والتعديل أو التدمير قد يسبب أضرار إلى الجامعة. وهي فرضت بأن كل الناتج الإداري من وسيلة استعمال الحاسبات المركزية صنفت بالحساسة إلا إذا حددت.

غير مقيد

المعلومات التي يمكن أن تُجعل متوفرة عموماً ضمن وما بعد الجامعة.

سياسة أمن البيانات

المعلومات الإدارية هي واحدة من ولاية جاكسون أكثر المصادر قيمة وتتطلب استعمالاً مسؤولاً من قبل أعضاء جالية الجامعة. مستخدمو ولاية جاكسون كلفوا بحماية السلامة، الدقة، وسرية هذه المعلومات كجزء من شرط العمالة.

المستخدمون يتوقعون التصرف وفق الأسلوب الذي سيضمن المعلومات التي يرخص لهم الوصول إليها محمية من دخول غير موثوق، استعمال غير موثوق، تغيرات باطلة، أو دمارها.

الدخول إلى الأنظمة الإدارية تُمنح إلى فرد معين مستندة على حاجة لاستعمال بيانات معينة، كما هو معرف من قبل واجبات الوظيفة، وبشرط الموافقة الملائمة. في حد ذاته، هذا الوصول لا يمكن أن يشترك فيه، يحوّل أو يفوض. الفشل لحماية هذه المصادر قد ينتج إلى إجراءات تأديبية تؤخذ ضد المستخدم، يعود إلى ويتضمن نتيجة.

مقدمة

بنود المعلومات وحماية البيانات يدوياً يفصّل مسؤوليات موظفي ولاية جاكسون في المحافظة على أمن المعلومات الإدارية. هؤلاء الأفراد هم أيضاً موضوع لسياسات احتوت في استخدام حاسبات المصادر في جامعة ولاية جاكسون بالإضافة إلى التعليمات المعينة للمعلومات الذي يصلون إليها. الأقسام التي تتلى تعرّف المسؤوليات، تؤسس الترخيص، وتزود المعلومات لمساعدة الناس في معالجة هذه المصادر- المعلومات.

الموظفين

مصطلح "موظف" يستخدم في هذا الدليل في معنى عام لدمج ليس فقط ناس دفعوا من قبل الجامعة لعملهم لكن أيضاً أولئك الذين يؤدون الخدمة لولاية جاكسون ويسمح لهم بالوصول إلى المعلومات الإدارية. المصطلح كما هو مستخدم هنا لا يمنح حالة خاصة أو علاقة مع الجامعة وليس المقصود منح حالة المستخدم. بالإضافة إلى الموظفين الدائمين والكلية، مصطلح موظف يشمل الموظفين المؤقتين، المستخدمين الطلاب، والاستشاريين، والمتطوعين، المساعدين، وزيارة الكلية.

المسؤوليات

المستخدمون مسؤولون عن أمن البيانات الإدارية. بينما هذه التعليمات تزود أمثلة العناية الملائمة، هم لم ينووا ليكونوا شاملين لكل النشاطات التي تضمن هذا الأمن. الموظفين توقعوا تقييم أعمالهم فيما يتعلق بحماية البيانات الإدارية والتصرف وفق أسلوب يكون أفضل اهتمام في الجامعة.

الطلبات للوصول إلى المعلومات الإدارية الإلكترونية يجب أن تصنع باستخدام الأشكال المناسبة في حزمة أشكال أنظمة المعلومات الإدارية المتوفرة من وسائل الاتصال المتاحة من قسم الكمبيوتر (منسقون المعلومات الإدارية أو القسم الذي يحسب المنسقون). متضمن على كل شكل أن يكون معلومات كافية ليحدد لماذا المستخدم يحتاج الوصول المطلوب وتواقيع طلب الإدارة المفوضة.

وفيما يلي يوجز مسؤوليات المستخدم:

- الامتناع من الدخول واستخدام المعلومات في الطرق الغير مرخصة المستخدمون الذين يحاولون الدخول الغير مرخص لهويات دخول الحاسوب الإداري يخضعون لإجراءات تأديبية. المستخدمون يجب أن لا يدخلوا إلى الحاسبات المصغرة التي لم تزود إليهم لعملهم بدون رخصة صريحة من مشرفيهم. هم مسؤولين أيضاً عن الامتناع من مطالعة البيانات الإدارية ليست المزودة لهم لعملهم. (حتى لو تركت في منطقة غير محمية) ومن دخول المناطق حيث المعلومات الإدارية خزنت إلا إن كان مرخص لهم.
- إتباع الإجراءات اللازمة لمخزن البيانات

  المستخدمون مطلوبين لإتباع إجراءات إدارية لتحديد أين يجب أن تخزن المعلومات الإدارية والإجراءات ارتبطت بتخزينها.

  مثل هذه الإجراءات تتضمن:
  - ضمان نسخ المعلومات الإدارية، مثل صورة وثائق مصغرة والمطبوعات في خزانة الملف أو المكتب.
  - تخزين المعلومات غير المنتجة في مناطق صممت لحمايتها من عرض غير مصرح وضرر من سبب طبيعي.
  - تخزين الأقراص المرنة في خزانة ملف مقفل أو مكاتب. أقراص بمعلومات حساسة يجب أن تقفل في الخزانة بقفل رئيسي غير قياسي.
  - نسخة احتياطية محلية تحفظ المعلومات الإدارية المخزنة على القرص لضمان تلك المعلومات بأن لا تفقد في حالة فشل القرص.
  - استبدال البيانات السرية المخزنة على قرص صلب في قطعة محمية ببرنامج أمن مصدق يطلب رقم سري للوصول.
- إتباع الإجراءات لانتشار البيانات

توزيع المعلومات الإدارية يجب أن ينجز خلال إجراءات مصدقة.

  - صون نشر المعلومات بالهاتف، فاكس، أو مواد مطبوعة لاستلام البيانات بمتابعة الإجراءات الإدارية التي تتوافق إلى سياسات أسست من قبل مسؤول بيانات حامي لتلك البيانات.

- تقل، عن طريق الشبكة، النسخ المحوسبة من البيانات الإدارية خلال إجراءات جامعة مصدقة. النسخ تنقل بالقرص المرن تتلي الإجراءات للانتشار الغير محوسب.

- إتباع الإجراءات للتخلص من البيانات

المستخدمون يجب أن يلتزموا بالإجراءات الإدارية لتحديد كيف يمكن التخلص من المعلومات الإدارية عندما لم يعد هناك حاجة إليها لأغراض العمل.

- تمزيق أو حرق الورقة أو نسخ صورة الوثائق لضمان أمن المعلومات.
- مراقبة الدليل في اختيار المستندات لتدمر.
- محو أشرطة مسجلة من (من جهاز تسجيل أو مسجلات): ليس فقط الكتابة فوقهم.
- رمي أقراص الحاسوب (أقراص صلبة أو مرنة) تحتوي على معلومات إدارية. يجب إعادة تهيئة أقراص ماك. أقراص الحاسوب الأخرى تتطلب أدوات متطورة لمنع الوصول إلى البيانات.

- حماية البيانات من دخول غير موثوق

المفاتيح وبطاقات الدخول اللذان يسرحان الدخول إلى مرافق التخزين حيث أن البيانات السرية مخزنة يجب أن لا تقرض أو تترك حيث يمكن للآخرين أن يستخدموهم للوصول إلى مناطق أمنة. كلمات السر هي المفتاح للدخول إلى خط المعلومات الإدارية.

- أبداً لا تقاسم كلمات السر حتى مع المشرف.
- اختيار كلمات السر التي ليست اختيار واضح. كلمات سر أخرى غير أسماء أفراد العائلة، ألقاب، كلمات موجودة في القاموس تجعلها أكثر صعوبة على شخص ما لاكتشاف كلمة السر.
- أبداً لا تسجل كلمات السر على الجدار، أو تحت لوحة المفاتيح، أو في مناطق أخرى تكشف بسهولة.
- تغيير كلمة السر كل ٩٠ يوم حتى لو لم يجبر النظام لذلك.

من أجل حماية المعلومات الإدارية المركزية من عرض غير مصرح به، يجب على محطات العمل تسجيل الخروج إلى نقطة تتطلب دخول جديد متى المستخدمون تركوا مناطق عملهم، ما عدا مناطق معينة خصيصاً. كل هويات الدخول يجب أن تسجل الخروج متى المستخدم غادر. يجب على المستخدمون أيضاً إتباع سياسات تتعلق بأمن طبيعي لمعدات الحاسوب.

يجب أن توجه الشاشات لمنع الناس الغير مصرح لهم من قراءة معلومات حساسة. موقع الشاشة يجب أن يوجه بعيداً عن أي مناطق مرور.

- الإبلاغ عن أي اختراق أمني

عندما يكون هناك خرق أمني فعلي أو مشكوك فيه يمكن أن يفضح المعلومات الإدارية، يجب الإبلاغ عن الحادثة فوراً للتحقيق من المشرف، مكتب أمن للمعلومات، أو مدقق الجامعة.

المشرفون

تعريف

يستخدم مصطلح "مشرف في هذا الدليل بحساسية عامة لدمج ليس فقط الناس الذين وظيفة عملهم تعرف لتشمل الإشراف على الموظفين، ولكن أيضاً لتوجيه الناس الذين يديرون عمل الآخرين. مثل هذه العناوين كمشرف، مدير، قائد، رئيس، رئيس قسم، عميد، ونائب الرئيس يستخدموا رسمياً ليدلوا على المشرف؛ على أية حال، العديد من المواقع تدل أيضاً على المشرف.

المسؤوليات

وهي مسؤولية المشرفين للحفاظ على مستوى عالي من الأمن في موقع العمل. المشرفون يتحملون المسؤولية لإبلاغ موظفيهم الأسلوب الصحيح لمعالجة المعلومات الإدارية، لتقييم فعالية هذه الإجراءات، ويوصوا بتغيرات لتحسين هذه الحماية. وبالإضافة إلى مسؤوليات الأمن المطبقة على جميع العاملين، والمشرفين لديهم مسؤوليات تتعلق بأمن البيانات على النحو المبين أدناه:

- مراجعة دخول موظفيهم

حاجة الموظفين لدخول المعلومات الإدارية كما هي محددة من قبل الرئيس/ رئيس القسم هي لتكون نتيجة المفاتيح، بطاقات الدخول، أو مجموعات المناطق حيث تحفظ المعلومات الإدارية ضمن تعليمات للدخول أسست من قبل الرئيس/ رئيس القسم. الأقفال الخاصة التي تزود مستوى عالي من الأمن غير أولئك المزودين من قبل صانعي الأثاث يمكن أن يحصلوا عليهم من عمليات النبات ويجب أن تستخدم لحماية المعلومات الإدارية الحساسة. المشرفون يجب أن يراجعوا الدخول الطبيعي لموظفيهم (على النحو المعرف من قبل إجراءات الإدارة) سنوياً على الأقل يجب على الموظفين أن يفترضوا مسؤوليات مختلفة ضمن الأقسام بمرور الوقت. المشرفون يجب أن يراجعوا كل الطلبات من قبل موظفيهم للوصول إلى معلومات إدارية إلكترونية. الطالبات يجب أن تقع ضمن تعليمات إدارية لوصول ملائم لتصدق. المشرفون يجب أن يراجعوا الدخول لكل عضو موظف بشكل دوري.

المشرفون أيضاً مسؤولون عن تزويد نسخ من هذه السياسة والدليل للتشاور، موظفين مؤقتين ومستخدمين خاصين آخرين ومساعدتهم كما هو محتاج لفهم السياسة.

- يضمن بأن المستخدمون امتثلوا للسياسات الأمنية والإجراءات

المشرفون يجب أن يعرّفوا ويشجعوا الموظف الذي هو واعي في المعالجة الصحيحة للمعلومات الإدارية. المشرفون يجب أن ينصحوا الموظف الذي انتهك إجراءات الأمن كما أوجزوا في قسم مستخدم هذا الدليل ومسؤولين عن تحسين الإدارة في سلوك الموظف. إذا استمرت الانتهاكات يجب أن تحل المشكلة.

- استخدام مراقب لتحديد المشكلة

يجب على المشرفون ضمان بأن نهاية عمل الموظف اليومي أمن المعلومات الإدارية ويجب مراقبة مناطق عمل الموظفين من الأشخاص الذين يحاولون التمكن من الوصول إلى مستندات تركت بلا رقابة. المشرفون أيضاً مسؤولون عن ملاحظة سلوك المستخدمين التي تشكل "التصفح" خلال البيانات ما بعد حاجات مواقعهم. تقارير الاستخدام ودخول إلى معلومات أخرى يجب أن تراجع من قبل المشرفين لضمان بأن الموظف يستخدم دخول صحيح. المشرفون يجب أن يبلغوا عن المشاكل إلى الرئيس/ رئيس القسم ومساعدة موظفين الجامعة في حل المشكلة.

- حذف الدخول عندما الموظف يترك القسم

المشرفون يجب ضمان بأن الموظفين الذين ينهون عملهم يجب أن يرجعوا مفاتيح الدخول والبطاقات في أخر يوم العمل في القسم. الموظف الذي يطرد من الجامعة يجب أن يرجع المفاتيح والبطاقات في الوقت الذي أبلغ بطردة. إذا هذا لم يحدث، يجب أن تلغى فوراً بطاقات الدخول ومواقع تحت سيطرة المفاتيح يجب أن تبرمج. عندما يفصل موظف من القسم أو يحول، يجب أن يبلغ لإغلاق دخوله في نهاية اليوم للمستخدم في القسم. على أية حال، عندما تتخذ الإجراءات التأديبية، يجب على المشرف أن يبلغ مكتب أمن المعلومات للاجتماع بالمستخدم من أجل إلغاء دخول الحاسوب خلال الاجتماع.

الرئيس/ رئيس القسم

تعريف

مصطلح رئيس/ رئيس قسم يستخدم ليدل على مدير الإدارة، أكاديمي أو البحث ضمن وحدة في الجامعة. هذا الشخص لدية مسؤولية مالية للقسم تتضمن تحضير الميزانيات ومراقبة التصرف. الرئيس/ رئيس القسم يبلغ مباشرة إلى مدير كبير.

المسؤوليات:

الرئيس/ رئيس القسم مسؤول عن تأسيس بيئة أمنة مطلعة على البيانات تستخدم بالقسم. هو يضع إجراءات تتعلق بأمن البيانات ودعم هذه الإجراءات بتوزيع الأموال.

الرئيس/ رئيس القسم يجب أن يراجع إجراءات المكاتب على الأقل على قاعدة سنوية وعمل تحديثات للرد على التغيرات في السياسات والتقنية.يجب أن تتوقع الميزانيات السنوية الحاجة لمصادر التمويل لحماية معلومات إدارية عينت في القسم. بالإضافة إلى مسؤوليات الأمن الملائمة لكل المستخدمين والمشرفين، الرئيس/ رئيس القسم لديه المسؤوليات التالية بخصوص أمن البيانات:

- ترجمة السياسات إلى إجراءات المكاتب

أمن البيانات وسياسة المعلومات الإدارية شملت في هذا الدليل شكلت قاعدة على أن إجراءات المكاتب يجب أن تطور لحماية المعلومات الإدارية. الإجراءات يجب أن تضمن بأن الدخول يزود بقاعدة معلومات تطلب لأداء العمل المخصص. الممارسات التي تعكس معالجة أنواع معينة أو تصنيفات البيانات التي يجب أن تضمن في ممارسات المكاتب.يجب أن تخاطب إجراءات المكاتب الحالات التالية :

- نقل الأشكال الغير إلكترونية للمعلومات الإدارية يجب أن تحفظ مستوى الأمن التي تضمن الأشخاص المصرح لهم فقط لمعالجة بيانات وصلوا إليها. الإجراءات يجب أن تتضمن قياسات معينة لحماية معلومات سرية ولتعقيب تدفق البيانات خلال القسم (للاقتراح، بواسطة السجلات).
- يجب تثبيت برنامج حماية من الفيروسات على كل الحاسبات الصغرى التي تحفظ المعلومات الإدارية لتحمي البيانات من التشويه أو الدمار.
- رؤساء/ رؤساء القسم يجب أن يضمنوا بأن صيانة الحاسوب اتخذت في سلوك لحماية سرية البيانات المخزنة في النظام. إن كان ذلك ممكنا، يجب أن تستخدم وسائل تصليح حاسوب جامعة ولاية جاكسون. إذا التجهيزات تطلبت استخدام وسائل تصليح خارجية، عقد الشراء للعمل يجب أن يتضمن عبارات غير مكشوفة تتعلق بمعلومات خزنت في قرص صلب و في النظام.
- الشبكات داخل القسم يجب أن تحمى لمنع دخول غير مصرح به.

- يزود المصادر لتنفيذ الإجراءات

- عندما لم يعد هناك حاجة لمعلومات إدارية غير إلكترونية في القسم، يجب أن تكون الآليات للتخلص من البيانات متوفرة. يجب أن تمزق المعلومات السرية في القسم أو تنقل بشكل أمن لتمزق أو تحرق بوسيلة صحيحة.
- مخزن (مؤقت أو دائم) من الأشكال الغير إلكترونية للمعلومات الإدارية يجب أن تحمى من عرض غير موثوق للمعلومات بالإضافة إلى الخسارة بسبب الحوادث أو أفعال طبيعية. الرئيس/ رئيس قسم يجب أن يزود وسائل تخزين كافية وقفل الأجهزة لضمان هذه الحماية.
- المعلومات الإدارية الحساسة أو الحرجة تحفّظ على الحاسوبات الصغرى يجب أن تبقى ضمن تقسيم إلكتروني الذي يتطلب كلمة سر للتمكن من الوصول. الرئيس/ رئيس قسم هو مسؤول عن ضمان بأن الأموال متوفرة لشراء برامج قابلة للقفل أو بأن المعلومات لم تبقى على قرص صلب.

- تحديد حساسية البيانات الغير مركزية التي نشأت في القسم

يجب أن يعرّف الرئيس/ رئيس قسم مستوى سرية المعلومات التي نشأت في القسم على أساس الوضع الحالي والقوانين الفيدرالية والتأثير المحتمل لخسارة تلك المعلومات حول سير العمل في الجامعة. استخدام الحاجة لمعرفة التعليمات، هو مسؤول عن تحديد نسر البيانات وتعليمها لمستخدميها في العناية الصحيحة للمعلومات الإدارية. البيانات التي تصنف بأنها غير مقيدة من قبل الرئيس/ رئيس قسم يجب أن تقع ضمن التعليمات التي وضعت للإطلاق من قبل علاقات مكاتب الجامعة قبل أن تنشر ما بعد ولاية جاكسون.

حماة مسؤولية البيانات

تعريف

حماية مسؤولية البيانات تشكل جسم للمستخدمين المعلمين الذي يعملوا كأوصياء المعلومات الإدارية للجامعة. لكل معلومات إدارية تحفظ مركزياً، المدير أو مدير وحدة وظيفية (القسم) تخصص السلطة لعمل قرارات تتعلق بتطوير، صيانة، عملية ودخول الطلبات وبيانات ارتبطت بوظيفة العمل.

حماة مسؤولية البيانات مسؤولون عن تأسيس تعليمات للإدارة وحماية هذه البيانات ولعمل التوصيات لتحسين توفر مصادر هذه الجامعة. كل حامي مسؤولية البيانات هو مسؤول عن مجموعة فرعية من المعلومات الإدارية الذي يحميها بالطرق التالية:

- الحفاظ على معرفة مفصلة للبيانات ضمن ثقتهم

حامي مسؤولية البيانات توقع أن يكون الشخص المعني بوظيفة العمل إلى ما تطبقه البيانات، التركيب ووظيفة إدارة أنظمة قاعدة البيانات في ما تستقر البيانات والطرق المتوفرة لدخول البيانات. يجب أن يكون حامي مسؤولية البيانات معني بالبيانات نفسها، تضمين قيم صحيحة وتحويلات البيانات، وأن يكون أيضاً قادراً على المساعدة بتحليل تغيرات الحقل وبتطبيق قوانين احتفاظ البيانات والممارسات.

- إدارة نشاطات تتعلق بعمل المعلومات

حامي مسؤولية البيانات يقيم، يصدق، ويعطي أولوية الطلبات للتغيرات إلى نظم العمل المسؤول عنه. بالإضافة ، أنه سوف يتصل إلى لجنة الحوسبة الإدارية في أي تغييرات رئيسية في ممارسات العمل التي تؤثر على قدرة الأنظمة لتستمر لتوفر خدمة ضرورية.

بالارتباط مع نظيرة وموظفي تقنية المعلومات، حماة مسؤولية البيانات يطورون التوصيات للجنة الحوسبة الإدارية بخصوص السياسات والإجراءات لإدارة معلومات العمل. هذه المجموعة أيضاً تنسق نشاط التخطيط المتعلق بحاجات عمل المناطق الوظيفية المختلفة.

حماة مسؤولية البيانات، مع توصيات الاحتساب ومعلومات الموظف، يساعد لجنة الحوسبة الإدارية بتطوير مدى بعيد لأهداف الحوسبة الإدارية وبترجمة هذه الأهداف إلى جداول لتبديل التطبيق أو فحص معين مع توصيات للأجهزة المتخصصة لدعم هذه التغيرات.

- تطوير تعليمات لطلب الدخول

استعمال ألفتهم بعناصر البيانات، حماة مسؤولية البيانات يترجمون مسؤولية العمل إلى قابلية الدخول لمساعدة المشرفين في تطوير التعليمات لدخول المستخدمين إلى البيانات. هذه التعليمات يجب أن تعكس أي حالة أو قوانين فدرالية في تحديد نشر المعومات بثقتهم.

- مراجعة الطلبات لدخول إلى المعلومات الإدارية

كل الطلبات للدخول إلى البيانات ائتمنت إلى حامي مسؤولية البيانات، كلاهما على الإنترنت وخلال الكمية، سوف يراجعوا و(١) يصدقوا، (٢) يعدلوا أو (٣) ترفض إبقاء التعليمات المؤسسة وممارسة الأمن العامة. حماة مسؤولية البيانات أو (مندوبيهم) سوف يخصصون دخول مستند على بيانات معينة التي تتطلب للمستخدم لينجز عمله.

- تعريف حساسية البيانات

كل حامي مسؤولية البيانات هو مسؤول عن تمييز عناصر البيانات أو مجموعات عناصر البيانات ضمن الثقة التي يجب أن تعالج مع مستوى عالي من الحماية وسرية إما بسبب الوضع أو قوانين فيدرالية تتحكم بالبيانات أو لأنها محددة من قبل دي آر أي بأنه في اهتمام الجامعة لإنتاج حماية خاصة للمعلومات. كل عناصر البيانات

فرضت لكي تصنف "بالحساسة" إلا إذا عينت بالجمهور من قبل حامي مسؤولية البيانات. هذا التصنيف سيستخدم لتعريف المعالجة الصحيحة للمعلومات في استخدام الموظف.

- تطوير التعليمات للمعالجة الصحيحة من المعلومات الإدارية

حماة مسؤولية البيانات سيطورون ويبقون تعليمات بخصوص الخلق، العرض، التعديل، التخزين، النقل، والتخلص من المعلومات الإدارية مستندة على مستوى حساسية البيانات. حيث الحالة أو القوانين الفيدرالية تملي معالجة خاصة لبعض البيانات، حامي مسؤولية البيانات يأتمن بالمعلومات التي ستضمن بأن الاستثناءات متضمنة في التعليمات.

- مراجعة معلومات مستخدمة

لتلك الأنظمة التي المعلومات في استخدام الأنظمة متوفرة، حامي مسؤولية البيانات مسؤول عن مراجعة التقارير المستخدمة لاكتشاف إساءة الاستعمال المحتملة من الدخول، تمييز المستخدمين الذين قد يحتاجون إلى تدريب إضافي في استعمال البيانات، استخلاص اتجاهات الاستخدام وملاحظة أي حالات شذوذ التي قد توضح البيانات ومشاكل الدخول. يعمل حامي مسؤولية البيانات مع ضابط أمن المعلومات لتوضيح وتصحيح أي مشكلة لحظت.

- المساعدة في تطوير الممارسات الأمنية الموحدة

حماة مسؤولية البيانات يساعدوا ضابط أمن المعلومات في تطوير الممارسات الأمنية في كافة أنحاء الجامعة وتعليم مستخدمين في هذه الممارسات. هذه الممارسات ستكون موثقة في دليل الأمن وتراجع من قبل حماة مسؤولية البيانات لضمان بأنها ملائمة في ضوء التغيرات في التقنية واتجاه الجامعة.

- المساعدة في التخطيط لاستئناف الأعمال

حماة مسؤولية البيانات، بالارتباط مع موظف تقنية المعلومات مسؤولون عن التطوير وإبقاء التخطيط اللذان سيسمحان لوظائف عمل الجامعة لتستمر في حالة توقف الخدمة. هذه الخطط لا تتضمن فقط القدرة على استعادة تطبيقات البرامج التي حفظت ولكن أيضاً وظيفة العمل التي أقيمت ضمن وحدة العمل نفسها.

لجنة الحوسبة الإدارية

تعريف

مصطلح "لجنة الحوسبة الإدارية" يشير إلى مجموعة ضباط يحددون الاتجاه، في النهاية ارتبطت السياسات بالحوسبة الإدارية. هؤلاء الضباط يتضمنوا الرئيس، نائب الرئيس لتقنية المعلومات، ونائب الرئيس للمالية أو ممثليهم المعينين.

المسؤوليات:

لجنة الحوسبة الإدارية لها مسؤولية لضمان حماية المعلومات الإدارية لولاية جاكسون، تأسيس السياسات والفلسفات للمعلومات وأمن البيانات وتخصيص مسؤوليات إلى مستخدمي الجامعة المختلفين لمساعدة اللجنة في هذه الأمور. مسئولياتهم فيما يتعلق بالمعلومات والأمن:

- مراجعة وتقييم الخطط لأنظمة المعلومات الإدارية

لجنة الحوسبة الإدارية لها المسؤولية لتنفيذ كل السياسات المتعلقة بإدارة عمل المعلومات. لجنة الحوسبة الإدارية، بمساعدة مسؤولية البيانات وموظف تقنية المعلومات، سوف يطورون خطط بعيدة المدى لأنظمة الحوسبة الإدارية ووضع أولوية لعكس أهداف الجامعة. لجنة الحوسبة الإدارية سوف يراجعون، ويقيّمون، ويصدّقون على صيانة معينة وخطط بديلة للأنظمة الإدارية بتوافق مع حاجات الحوسبة للجامعة وتوفر المصادر المالية. هي أيضاً مسؤولية لجنة الحوسبة الإدارية لمراجعة وتقييم تقدم هذه الخطط.

- مراجعة وتصديق السياسات

لجنة الحوسبة الإدارية هي مسؤولة عن مراجعة وتصديق سياسة المعلومات وأمن السياسة لضمان بأن هذه السياسات تكملة والتزام بفلسفات العمل لولاية جاكسون. أي تعديلات لهذه السياسات يجب أن تراجع وتصدق من قبل هذه اللجنة.

- مراجعة ضوابط الأمن

لجنة الحوسبة الإدارية تراجع الفلسفات وخطط عامة تسيطر على الأمن واستخدام المراقبة. هذه المجموعة تشرف على حماية المعلومات الإدارية أثناء إبقاء الحقوق الفردية للمستخدمين ووضع أولويات لخطط الأمن فيما يتعلق بالموارد الحالية والمتوقعة.

- توفير الوسائل لتطبيق السياسات

لكي تكون السياسات فعالة، يجب أن يكونوا موحدين في بيئة العمل. لجنة الحوسبة الإدارية خلال إجراءات مختلفة، تسهل تطبيق هذه السياسات. اللجنة هي مسؤولة عن تحديد مصادر المالية لتطبيق سياسات وإجراءات حسب الضرورة.

- تنفيذ السياسات

في حالة اختراق أمني خطير، أعضاء لجنة الحوسبة الإدارية سوف يراجعون التقارير والدليل (ضمن اجتماع السامعين للضرورة) لتحديد المذنب وتوضيح تعرض الجامعة للخرق، اتخاذ خطوات للتقليل من تعرض الجامعة للخرق، تقليل من احتمال خرق مماثل في المستقبل، وعند الاقتضاء يقرر ما الإجراء التأديبي الذي سيأخذ.

- توضيح وتفسير السياسات

أسئلة تعلقت بمجال أو بتطبيق السياسات يجب أن تعود إلى لجنة الحوسبة الإدارية للحل. على الرغم من أن حماة مسؤولية البيانات وضباط أمن المعلومات هم الاتصالات الأساسية لهذه الأنواع من الأسئلة، ويمكن أن يسألوا أعضاء لجنة الحوسبة الإدارية ليراجعوا إجراءات متعلقة بفلسفات عمل المؤسسة.

- ضمان بأن تبقى السياسات على حالها

كتقنيات وممارسات تطور في ولاية جاكسون، لجنة الحوسبة الإدارية هي مسؤولة عن ضمان سياسة ملائمة تحمي الجامعة. عندما تحتاج السياسات لتراجع لمقابلة التغييرات، لجنة الحوسبة الإدارية ستنسب هذه المسؤولية لموظف جامعة متخصص.

المدققين الداخليين

تعريف

يستخدم "مدقق داخلي" في هذا الدليل ليشير إلى مدقق الجامعة وأعضاء آخرين من موظفي التدقيق الداخلي. وهو غير قابل للتطبيق إذا لم يكن من مستخدمين ولاية جاكسون. يزود المدققين الداخليين وجهة نظر موضوعية ومستقلة إلى الجامعة على الأمن لمصادر معلوماته.

المسؤوليات:

بموجب دستور مدقق الجامعة، مدققين داخليين لولاية جاكسون هم مصدّقون لتحقيق دخول لكل الأنظمة والمعلومات الإدارية، ومسؤولون عن مساعدة المشرفين في تأدية واجباتهم بفعالية. بالإضافة إلى أن يكون موضوع سياسات أمن المعلومات قابل للتطبيق من قبل مستخدمين آخرين لولاية جاكسون، يجب على المدققين الداخليين لولاية جاكسون المصدق عليهم أن يلتزموا بتدقيق المعايير والرموز التي أسست من قبل مجموعات ملائمة مصدق عليها. في ممارسة واجباتهم المتعلقة بأمن المعلومات والمدققين الداخليين:

- تقييم الامتثال لسياسة أمن المعلومات والإجراءات ضمن أقسام الجامعة أثناء تدقيق عملي وإداري.
- تقييم فعالية إجراءات الأمن وسيطرة داخلية لدخول محدد إلى المعلومات الإدارية المخصصة وتحديد واقتراح التحسينات لمناطق الضعف.
- مراجعة آثار تدقيق الحسابات المزودة من قبل أنظمة تطبيق الأمن لتقييم إذا نشاط موثق بشكل كافي يسمح للأخطاء ويحدد الأخطاء، لتتبع مصدرها وتصحح.
- يساعد الإدارة في التحقيق في حوادث مشبوها لاختراق الأمن أو نشاط غير لائق.
- تزويد نصيحة على السيطرة الداخلية ذات العلاقة لتجديد الأنظمة لتكون متطورة أو تعتبر للشراء.

حوسبة الخدمات وموظف تقنية المعلومات

المسؤوليات

حوسبة الخدمات وموظف تقنية المعلومات لديهم الخبرة والمسؤولية لحماية المعلومات الإدارية المقيمين على الحاسبة الإلكترونية للجامعة، شبكة، وخادمات محلية ويجب أن تستخدم هذه الخبرة في أخلاق المسؤولية لضمان سلامة البيانات وتوافر المعلومات. بسبب فرصتهم الكبيرة لدخول المعلومات الإدارية، موظف تقنية المعلومات وحوسبة الخدمات لدية مسؤوليات إضافية.

- التقيد باتفاق عدم الكشف عن القسم

كل مستخدم في تقنية المعلومات والحوسبة الإدارية يجب أن يقرأ ويوقع بيان غير مكشوف كشرط للتوظيف. يجب أن يتبع الموظفون قيود وضعت فوقهم من الاتفاقات بالإضافة إلى السياسة على أمن المعلومات.

- الحفاظ على البيانات والبرامج ضمن معايير مؤسسة

كل بيانات تحدد أسماء يجب أن توافق مع اصطلاحات التسمية اتخذت من قبل تقنية المعلومات وحوسبة الخدمات. الموظفون لن يعيدوا تسمية أو إنشاء بيانات وضعت مع عكس الأسماء للمعايير للنيل من أمن يحمي هذه المصادر.

البرامج ستطور أو تعدل معايير تالية أسست من قبل القسم. وأيضاً ستلاحظ آليات موحدة لتوثيق التغيرات.

- توفير الأمن لأنظمة الحاسوب

موظف الحوسبة هو مسؤول عن إجراءات القسم التالية فيما يتعلق بالحماية الطبيعية للأجهزة في أنظمة حاسوب ولاية جاكسون. هذا يتضمن (ولكن ليس محدد إلى) حاسبات كبرى وصغرى، محطات العمل، الخادمات، الطابعات، أجهزة تخزين خارجية، المودمات وأي مكونات أجهزة أخرى بالإضافة إلى الشبكة الطبيعية التي تضم هذه الآلات. حيث أن دخول طبيعية حدد من قبل أجهزة الأمن، الموظفين لن يشاركوا دخولهم "المفاتيح" أ، النيل من أجهزة الأمن. الزوار إلى مناطق أمنة حيث يتم إيواء معدات الحاسوب يجب أن تواكب من قبل موظف القسم، الذي يفترض جنباً إلى الزوار، مسؤولية لطبيعة ومنطقية سلامة الآلات خلال تلك الفترة.

كجزء من وقاية أنظمة الحاسوب، نسخة احتياط عادية ستنتج لسماح إعادة بناة الأنظمة في حالة ضرر الملف أو الأجهزة. هذه النسخ ستخزن في مواقع مختلفة من أجهزة الأنظمة وحرم الجامعة لأنظمة الأعمال الحرجة.
برنامج النظام سيطبق أو يعدل بإتباع إجراءات معرفة من قبل البائع للأجهزة التي تستقر فيها. أي "فيروس" سيصلح بأسرع وقت ممكن من قبل موظف الأنظمة، إذا كان ذلك مناسباً، سيبلغ المستخدمون بالأخطاء المحتملة التي تسبب الخطأ.
قواعد البيانات الإدارية ستدار بإتباع معايير مقبولة تتضمن مراجعة مساحة متوفرة لضمان وجود مناطق كافية، إدراج قيمة تصحيح البيانات في برامج إدخال البيانات، وتفعيل استخدام آليات الإبلاغ، والإنتاج المنتظم ومراجعة استخدام التقارير.

- المساعدة بتطوير خطط بعيدة المدى

موظفو تقنية المعلومات سيساعدون حماة مسؤولية البيانات سيطورون توصيات إلى لجنة الحوسبة الإدارية عن أهداف الحوسبة الإدارية البعيدة المدى. سيساعدون أيضاً بترجمة هذه الأهداف إلى جداول لتبديل التطبيق وفحص رئيسي بالإضافة إلى التوصيات للأجهزة المخصصة لدعم هذه التغيرات.

- التدريب والتشاور مع الحوسبة الإدارية

أقسام الشبكات الإدارية، منسقو الحوسبة الإدارية وحماة مسؤولية البيانات يساعدوا على الاتصال بين أقسامهم وخدمات الحوسبة المركزية. تقنية المعلومات وخدمات الحوسبة تزود تدريب خاص لهذه الوظائف لإبقاء مستوياتهم من الكفاءة عندما تغير التقنيات. بالإضافة، تقنية المعلومات وموظفي خدمات الحوسبة تدعم جهد الحوسبة ضمن القسم بالرد على أسئلتهم ومشاكلهم.

- المساعدة بتطوير خطط استئناف العمل

موظف تقنية المعلومات، بالتعاون مع حماة مسؤولية البيانات سيطورون ويحفظون الخطط التي تعيد الخدمات إلى أجهزة مركزية وأنظمة برنامج التطبيق في حالة توقف الخدمة. الخطة ستتضمن معلومات للمساعدة في تحديد السلسة لإعادة تطبيقات الأعمال الحرجة.

ضابط أمن المعلومات

المسؤوليات:

ضابط أمن المعلومات مسؤول عن تأسيس ومراقبة الإجراءات لضمان بأن المعلومات الإدارية لولاية جاكسون حميت من دخول غير مصرح به، حميت من تعديل خاطئ ومتوفرة لدى مستخدمين موثقين بطريقة مناسبة لتمكينهم من أداء واجباتهم. متضمن في هذه المسؤوليات الضرورة ليكون الفني فصيح بالأنظمة الأمنية المختلفة تستخدم لحماية البيانات وللتعويض باستخدام الإجراءات، لأي عيوب لهذه الأنظمة. هذه المسؤوليات تتضمن التالي:

- تطوير وإبقاء إجراءات أمن فعالة

ضابط أمن المعلومات مسؤول عن التطوير، بالتعاون مع حماة مسؤولية البيانات، الإجراءات لتطبيق سياسات أمن بيانات الجامعة. جزء مهم من هذه المهمة لمراجعة كل تقارير الدخول والسجلات. ضابط أمن المعلومات سيعمل مراجعة في كافة أنحاء النظام للدخول تزود للمستخدمين لضمان بأن الدخول ثابت مع التعليمات المؤسسة للأنظمة وبأن التعليمات تزود دخول ضروري. كأنظمة جديدة أو معدلة قدمت، ضابط أمن المعلومات يعمل مع حامي مسؤولية البيانات لمراجعة تطوير الإجراءات لحماية المعلومات وتوثيق الدخول. هذه الإجراءات يجب أن تتضمن آليات ل:

  - يعوض لنقائص النظام الأمني.
  - التقارير على نشاط النظام
  - تزويد المستخدمين دخول إلى البيانات
  - نشر معلومات إلى المستخدمين على المعالجة الملائمة للبيانات
  - تدمير النسخ الغير إلكترونية من المعلومات

لأنظمة موجودة، ضابط أمن المعلومات بالتعاون مع حماة مسؤولية البيانات، وفريق التطوير يراجعوا إجراءات حالية للتحقق بأنهم زودوا مستوى كافي من الحماية وحسب الحاجة، تعمل توصيات لجلبهم إلى الالتزام بمعايير مقبولة من الأمن.
إذا حدث خرق في نظام الأمن، ضابط أمن المعلومات سيراجع التعليمات وإجراءات النظام وإذا كان ضروري، يوصي بتغيرات لتحسين حماية بيانات الجامعة.
للأنظمة التي سلمت بدون آليات كاملة لنشاط التقارير، ضابط أمن المعلومات سيعمل مع فريق تطوير مناسب لتعريف البيانات لتحفظ وسلوك التقارير.

- اختبار وتوثيق أنظمة أمنية إدارية

استخدام إجراءات اختبار قياسية، ضابط أمن المعلومات مسؤول عن تحديد مجال الأمن زودت من قبل أنظمة احتياطية استعملت في ولاية جاكسون لحماية المعلومات الإدارية وتوثيق هذه الأنظمة. متضمن في هذا التوثيق أي قيود، شذوذ، عيوب وهتك.

- الاستشارة على القضايا الأمنية الداخلية

ضابط أمن المعلومات مسؤول عن نصح حماة مسؤولية البيانات، مدققين داخليين، وإدارة عليا تتعلق بأشغال التقنية لأنظمة الأمن الفرعية للأنظمة الإدارية.
هو أيضاً يتشاور مع المطورين، تدعم الأنظمة الموظفين والمستعملين لضمان بأن ميزة الأمن الكافية متضمنة في برنامج أنظمة المعلومات الجديدة والمعدلة.

- تحضير واحتفاظ بسياسات أمن عامة وتعليمات

ضابط أمن المعلومات مسؤول عن إنتاج وإبقاء سياسات أمن البيانات للجامعة لتراجع ويوافق عليها من قبل حماة مسؤولية البيانات، لجنة الحوسبة الإدارية، والإدارة العليا في الجامعة. دعم التوثيق لهذه السياسات يطور من قبل ضابط أمن المعلومات بالتعاون مع حماة مسؤولية البيانات وكتقنيات وسياسات متطورة، محتوياتهم تحدث من قبل ضابط أمن المعلومات. ضابط أمن المعلومات يساعد حماة مسؤولية البيانات في تطوير وإبقاء التعليمات للمعالجة الصحيحة واستخدام المعلومات الإدارية في مجالهم. يساعد في نشر هذه التعليمات إلى القسم الذي يستخدم البيانات. ضابط أمن المعلومات يمكن أن يساعد أيضاً الرؤساء/ رؤساء القسم في تطوير إجراءات إدارية لتطبيق تعليمات معينة أسست من قبل حماة مسؤولية البيانات.

- تزويد المساعدة بتدريب الأمن

ضابط أمن المعلومات مسؤول عن تزويد معلومات لتدريب وعي الأمن العام مثل التعليم المعين على سياسات أمن الجامعة ودليل الأمن. هو قد يساعد أيضاً الرئيس/رئيس القسم في تحضير تدريبات المواد لموظفيهم على إجراءات الأمن الإدارية. هي مسؤولية ضابط أمن المعلومات ليساعد في تفسير السياسات المتعلقة بالحالات المعينة التي تظهر ومساعدة المستخدمين ليكونوا قادرين على اتخاذ قرارات متسقة بهذه السياسات.

- مراجعة مخزن دخول البيانات

لكي تحدد مجموعات الدخول كل مستخدم عنده معلومات إدارية، ضابط أمن المعلومات مسؤول عن تخزين معلومات تحتوي على امتيازات لكل مستخدم عبر الأنظمة الإدارية. هذه المراجعة تضمن بأن المستخدمين لديهم دخول يحتاجوه لأداء عملهم وبأن دخولهم العام على التزام بتعليمات عامة من الأمن.

مدراء هوية الدخول

المسؤوليات

مدراء هوية الدخول هم مستخدمين ولاية جاكسون، لمن تضمن واجباتهم الإنشاء، الحذف، أو تعديل هويات الدخول أو صيانة هوية جداول الدخول التي تتحكم بالقدرة لعرض أو تحديث المعلومات الإدارية. بسبب مجال هذه القابلية، مسؤوليات إضافية خصصت لدخول هوية المدير كالتالي:

- المحافظة على توثيق كامل لكل التغييرات

قبل أي هوية دخول أو إذا عدلت الجداول، كتابة التوثيق يجب أن تكمل التي تحتوي على تواقيع أصلية لمالك هوية الدخول، مشرفيهم وحماة مسؤولية البيانات الملائمة. في الظروف الخاصة، بريد الكتروني يسمح في مكان الأشكال الموقعة؛ هذه الاستثناءات ستراجع وتوثق قبل التطبيق. مدراء هوية الدخول مسؤولين عن المحافظة على توثيق التغيرات لأغراض التدقيق. خصوصاً في الحالات التي يشغل حامي مسؤولية البيانات كدخول هوية المدير، أي تغيرات لهوية الدخول يجب أن تراجع من قبل رئيس المعلومات للتطبيق.

- تنفيذ دخول عرف من قبل حامي مسؤولية البيانات

مدراء هوية الدخول يجب أن يحولوا بدقة الدخول المعرف من قبل حماة مسؤولية البيانات في تعريف هوية الدخول. إذا كان تعريف الدخول غير واضح أو متضارب، مدير هوية الدخول سيرجع الطلب إلى حامي مسؤوية البيانات للتوضيح.

- تعليق الدخول عندما ينتهي أو يحول المستخدم

استخدام معلومات زودت من قبل مكتب الموارد البشرية، مدراء هوية الدخول سيحذفون هويات المستخدمين الذين فصلوا من الجامعة وستقفل أو تحذف هويات المستخدمين الذين حولوا إلى أقسام أخري ضمن ولاية جاكسون. عندما تصنع ترتيبات خاصة للمستخدم ليكون لديه دخول ما بعد يومه الرسمي الأخير في القسم، مدراء هوية الدخول سيحددون تاريخ الانتهاء على هوية الدخول (إذا يسمح الأمن) أو سيحافظ على "مذكرة" الملفات لتذكيرهم بحذف هوية الدخول في نهاية فترة الامتداد.

تغيرات النظام

- نظام الإنتاج

كل التغيرات التي اقترحت لبيئة الإنتاج يجب أن تصدق من قبل إدارة عالية المستوى. أي فرد أو مجموعة يتأثروا بهذه التغيرات يجب أن يبلغ عنها في كتابة سابقة للتغيرات التي اتخذت. يجب أن تصنع التغيرات في بيئة الاختبار ويثبتوا قبل أن يوضعوا إلى الإنتاج. تغيرات نظام التطبيق يجب أن تصدق من قبل ذلك حامي الأنظمة وعضو موظف مركز الحاسوب الذين هم صنعوا. يصدق مرة واحدة، هذه التغيرات يجب أن تركب في بيئة الاختبار وأن تختبر من قبل موظفي مركز الحاسوب وجالية المستخدم قبل أن توضع إلى الإنتاج.

- اتصالات البيانات

التغيرات المقترحة إلى تركيبة شبكات الجامعة قبل أن تصدق من قبل إدارة مراكز الحاسوب قبل أن تصنع. كل التغيرات يجب أن تصنع أولاً في بيئة الاختبار حيث التغيرات تختبر وتحقق لتكون صحيحة من قبل شخص يطلب التغير وأعضاء موظفي تقنية المعلومات.

ملحق أ – معاني المصطلحات

مدير هوية الدخول:

مدير هوية الدخول هو مستخدم واجباته تتضمن إنشاء، حذف، أو تعديل هويات الدخول أو صيانة جداول هويات الدخول التي تتحكم بالدخول إلى المعلومات الإدارية.

لجنة الحوسبة الإدارية:

مصطلح "لجنة الحوسبة الإدارية يشير إلى مجموعة من ضباط كبار يقرروا اتجاهات وسياسات ترتبط بالحوسبة الإدارية.

منسق المعلومات الإدارية:

منسق المعلومات الإدارية مسؤول عن عملية دقيقة وانتهازية من المعلومات التي احتاجت للجامعة. المنسق يمثل قسمه في مادة تتعلق ببيئة الإنتاج الإدارية باجتماع منتظم على مدار السنة مع موظف الدعم الإداري في تقنية المعلومات.

الرئيس/ رئيس القسم:

مصطلح رئيس/ رئيس قسم يدل على مدير إداري، أكاديمي أو وحدة بحوث ضمن الجامعة. هذا الشخص لديه مسؤولية مالية للقسم تتضمن تحضير ميزانيات ومراقبة الصرف. الرئيس/ رئيس القسم يبعث تقارير مباشرة إلى الإدارة العليا.

بيانات سرية:

المعلومات التي تتطلب مستوى عالي من الحماية بسبب الخطر و مقدار الخسارة أ، الضرر التي تنتج من الكشف أو التعديل أو تدمير البيانات. هذا يتضمن معلومات من حيث أن استخدام غير صحيح أ، الكشف عنها يمكن أن يؤثر على قدرة الجامعة لإنجاز المهمة بالإضافة حول أفراد يطلبون حماية تحت الحقوق التربوية العائلية وحماية سرية من ١٩٧٤ وبيانات غير مبعثه تحت قانون حرية المعلومات.

حامي مسؤولية البيانات:

حماة مسؤولية البيانات يشكلون جسم من المستخدمين المطلعين الذين يعملون كأوصياء للمعلومات الإدارية. لكل تطبيق إداري يحفظ مركزياً، المدير أو مدير وحدة وظيفية في (القسم) يخصص السلطة لصنع القرارات المتعلقة بالتطوير، الصيانة، الدخول وعملية التطبيق وارتبطت البيانات بوظيفة العمل.

منسق استخدام حاسبات القسم:

منسق استخدام حاسبات القسم هو موظف أو تلميذ متخرج خصص من قبل القسم لتزويد دعم الحاسوب المخصص في بيئة القسم.

المشرف على الشبكة الإدارية:

المشرف على الشبكة الإدارية مسؤول عن دعم بيئة الشبكات في القسم. تتضمن المسؤوليات في تثبيت التطبيقات على خدام الإدارة وتزويد دعم أول مستوى و أسئلة تتعلق بمشاكل الشبكة.

المستخدم:

مصطلح "مستخدم" يستعمل لغرض هذا البيان لدمج ليس الناس الذين دفعوا من قبل الجامعة لعملهم ولكن أيضاً هؤلاء الذين أدوا بعض الخدمات لولاية جاكسون ويسمح للدخول إلى المعلومات الإدارية.

المدقق الداخلي:

يستخدم هذا المصطلح للإشارة إلى مدقق الجامعة وأعضاء آخرين من موظفي تدقيق الحسابات.

ضابط أمن المعلومات:

ضابط أمن المعلومات مسؤول عن تأسيس ومراقبة الإجراءات لضمان أن المعلومات الإدارية لولاية جاكسون أمنة من دخول غير مصرح به، محمية من التعديل الخاطئ ومتوفرة لمستخدمين مصرح لهم لتمكينهم من أداء أعمالهم.

البيانات العامة:

المعلومات التي يمكن أن تكون متوفرة ضمن وما بعد الجامعة.

الأمن :

المعلومات تكون أمنة فقط عندما تحفظ سلامتها، وتوافرها مضمون، وتحفظ سريتها ويتحكم بدخولها.

البيانات الحساسة :

المعلومات التي تتطلب بعض مستويات من الحماية وذلك لأن الكشف عنها غير مصرح به ، وأي تغيير، أو تدمير يلحق أضرراً بالجامعة.

المشرف :

مصطلح "المشرف" لا يدمج فقط الناس المعرف عملهم، لضمان الإشراف على الموظف ولكن يستعمل للناس الذين يديرون عمل الآخرين.

ملحق ب – التصنيفات البديلة للبيانات

مخططات التصنيفات تزود وجهات نظر بديلة إلى تصنيفات استخدمت لأمن البيانات. الأبعاد الثلاثة- الوظيفة، المجال، الأهداف تصنف البيانات بشكل يشجع تسلقها نموذجياً، بانتظام، وطريق صحيح. إن هدف خطط التصنيفات هو لضمان استقلالية البيانات من الهيكل التنظيمي وبرنامج التطبيق.

المناطق الوظيفية:

المنطقة الوظيفية معرفة بغرض الجامعة الأساسي خدمت من قبل البيانات. وهي لا تتبع خطوط تنظيمية من السلطة. بسبب تكامل واسع عبر الوحدات الوظيفية، تصنيف وظيفي قد يكو اختياري. وحدة الوظيفة قد تعطي سلطة للبيانات المشتركة من قبل العديد من وحدات تنظيمية أخرى. تصنيفات المنطقة الوظيفية:

بيانات الطالب:

بيانات الطالب تدعم كل مراحل علاقة الطلاب مع الجامعة من التطبيقات خلال حالة الخريجين، ما عدا التي لوحظ في مكان ما. هذه يتضمن (لكن لم يحدد إلى) بيانات سكانية، سجلات أكاديمية، تأديبي، وسجلات صحية، دورة المعلومات، قبول البيانات، المالية، وبيانات طلاب غير مالية ومعلومات التطوير.

البيانات المالية:

تدعم البيانات المالية إدارة المصادر المالية للجامعة وتضمن المحاسبة، وضع ميزانيات، استثمارات، قروض.

بيانات الموارد البشرية:

تدعم بيانات الموارد البشرية إدارة مصادر المستخدم للجامعة وتتضمن كل أنواع المعلومات المتعلقة بالمستخدم كما عرفت مسبقاً. وهذه البيانات تتضمن المستخدم، الديموغرافيه، التقاعد، تقييمات المستخدم، المندوب وبيانات تأديبية.

بيانات شؤون العمل:

تدعم بيانات شؤون العمل مشاريع الجامعة مثل مبيعات جزئية، تجهيزات مركزية، خدمات تخطيطية، واتصالات.

المصادر والمراجع :

١-موسوعة ويكيبيديا .

٢-عدد من رسائل الماجستير مرفقه على السي دي .