IT Policies and Procedures

Versioning

Date	Changes	Modified by
15 January 2018	Initial Document	Ginanjar Fahrul M
1 March 2018	Add BYOD policy	David Samuel

Introduction

The Ritase IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the institution which must be followed by all staff. It also provides guidelines Ritase will use to administer these policies, with the correct procedure to follow.

Ritase will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

Technology Hardware Purchasing Policy

Policy Number: RPC-A001
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives and RAM. External hardware devices include monitors, keyboards, mice, printers and scanners.

Perkenalan

Manual Kebijakan dan Prosedur TI Ritase memberikan kebijakan dan prosedur untuk pemilihan dan penggunaan TI dalam institusi yang harus diikuti oleh semua staf. Ini juga memberikan pedoman yang akan digunakan Ritase untuk mengelola kebijakan ini, dengan prosedur yang benar untuk diikuti.

Ritase akan menjaga semua kebijakan TI terkini dan relevan. Oleh karena itu, dari waktu ke waktu perlu untuk mengubah dan mengubah beberapa bagian dari kebijakan dan prosedur, atau untuk menambah prosedur baru.

Setiap saran, rekomendasi, atau umpan balik mengenai kebijakan dan prosedur yang ditentukan dalam manual ini dipersilahkan.

Kebijakan dan prosedur ini berlaku untuk semua karyawan.

Kebijakan Pembelian Perangkat Keras Teknologi

Nomor kebijakan: RPC-A001

Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Perangkat keras komputer mengacu pada bagian fisik komputer dan perangkat terkait. Perangkat perangkat keras internal termasuk motherboard, hard drive dan RAM. Perangkat perangkat keras eksternal termasuk monitor, keyboard, mouse, printer, dan scanner.

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the institution to ensure that all hardware technology for the institution is appropriate, value for money and where applicable integrates with other technology for the institution. The objective of this policy is to ensure that there is minimum diversity of hardware within the institution.

Procedures

Purchase of Hardware

The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy.

Purchasing desktop computer systems

There is no desktop purchase policy. Workstation for all employee is applied by BYOD policy.

Purchasing portable computer systems

There is no portable purchase policy. Workstation for all employee is applied by BYOD policy.

Purchasing server systems

Server systems can only be purchased or registered by IT Specialist. Server systems must be compatible with all services running in the institution.

All purchases of server systems must be supported by warranty and be compatible with the institution’s other systems.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk pembelian perangkat keras bagi institusi untuk memastikan bahwa semua teknologi perangkat keras untuk institusi tersebut sesuai, bernilai uang dan jika dapat diintegrasikan dengan teknologi lain untuk institusi tersebut. Tujuan kebijakan ini adalah untuk memastikan bahwa ada keragaman perangkat keras minimum di dalam institusi.

Prosedur

Pembelian Perangkat Keras

Pembelian semua desktop, server, komputer portable, periferal komputer, dan perangkat seluler harus mematuhi kebijakan ini.

Pembelian Sistem Komputer Desktop

Tidak ada kebijakan pembelian desktop. Workstation untuk semua karyawan diterapkan oleh kebijakan BYOD.

Pembelian Sistem Komputer Portabel

Tidak ada kebijakan pembelian portabel. Workstation untuk semua karyawan diterapkan oleh kebijakan BYOD.

Pembelian Sistem Server

Sistem server hanya dapat dibeli atau didaftarkan oleh Spesialis TI. Sistem server harus kompatibel dengan semua layanan yang berjalan di institusi.

Semua pembelian sistem server harus didukung oleh garansi dan kompatibel dengan sistem lain institusi.

Any change from the above requirements must be authorised by IT Head Department.

All purchase for server systems must be in line with the purchasing policy in the Financial Policies and Procedures Manual.

Purchasing computer peripherals

Computer system peripherals include printers, scanners, external hard drives and any other work-relevant hardware.

Computer peripherals can only be purchased when employees require supported peripherals for their BYOD workstation and the peripherals can be shared with other employees.

Computer peripherals must be compatible with all other BYOD workstations.

The purchase of computer peripherals can only be authorised by IT Specialist.

All purchases of computer peripherals must be supported by warranty and be compatible with the institution's other systems.

Any change from the above requirements must be authorised by IT Head Department.

All purchase for computer peripherals must be in line with the purchasing policy in the Financial Policies and Procedures Manual.

Purchasing mobile telephones

There is no mobile telephones policy. Mobile telephones for all employee is applied by BYOD policy.

Setiap perubahan dari persyaratan di atas harus disahkan oleh Kepala Departemen TI.

Semua pembelian untuk sistem server harus sejalan dengan kebijakan pembelian dalam Manual Kebijakan dan Prosedur Keuangan.

Pembelian peripheral komputer

Periferal sistem komputer mencakup printer, pemindai, hard drive eksternal, dan perangkat keras lain yang terkait dengan pekerjaan.

Periferal komputer hanya dapat dibeli ketika karyawan membutuhkan periferal yang didukung untuk stasiun kerja BYOD mereka dan periferal dapat dibagikan dengan karyawan lain.

Periferal komputer harus kompatibel dengan semua workstation BYOD lainnya.

Pembelian peripheral komputer hanya dapat diotorisasi oleh Spesialis IT.

Semua pembelian periferal komputer harus didukung oleh garansi dan kompatibel dengan sistem lembaga lainnya.

Setiap perubahan dari persyaratan di atas harus disahkan oleh Kepala Departemen TI.

Semua pembelian untuk periferal komputer harus sejalan dengan kebijakan pembelian dalam Manual Kebijakan dan Prosedur Keuangan.

Pembelian Telepon Seluler

Tidak ada kebijakan telepon seluler. Telepon seluler untuk semua karyawan diterapkan oleh kebijakan BYOD.

Purchasing system infrastructure policy

System infrastructure used at any Infrastructure as a Service (IaaS) can be purchased in order to maintain server system.

The purchase of system infrastructure license can only be authorised by IT Specialist.

All purchases of system infrastructure must be supported by warranty, reputable system infrastructure provider and be compatible with the institution's other systems.

Any change from the above requirements must be authorised by IT Head Department.

All purchase for computer peripherals must be in line with the purchasing policy in the Financial Policies and Procedures Manual.

Policy for Getting Software

Policy Number: RPC-A002
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the institution to ensure that software used by the institution is appropriate, value for money and where applicable integrates with other technology for the institution. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

Pembelian Kebijakan Infrastruktur Sistem

Infrastruktur sistem yang digunakan pada Infrastruktur sebagai Layanan (IaaS) dapat dibeli untuk memelihara sistem server.

Pembelian lisensi infrastruktur sistem hanya dapat diotorisasi oleh Spesialis IT.

Semua pembelian infrastruktur sistem harus didukung oleh garansi, penyedia infrastruktur sistem yang memiliki reputasi baik, dan kompatibel dengan sistem lembaga lainnya.

Setiap perubahan dari persyaratan di atas harus disahkan oleh Kepala Departemen TI.

Semua pembelian untuk periferal komputer harus sejalan dengan kebijakan pembelian dalam Manual Kebijakan dan Prosedur Keuangan.

Kebijakan untuk Mendapatkan Perangkat Lunak

Nomor kebijakan: RPC-A002
Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk pembelian perangkat keras bagi institusi untuk memastikan bahwa perangkat lunak yang digunakan oleh institusi sesuai, nilai uang dan jika dapat diintegrasikan dengan teknologi lain untuk institusi. Kebijakan ini berlaku untuk perangkat lunak yang diperoleh sebagai bagian dari bundel perangkat keras atau perangkat lunak yang dimuat sebelumnya.

Procedures

Request for Software

All software, including non-commercial software such as open source and freeware software are adjusted based on needs. For all software installed at server systems must be approved by IT Specialist prior to the use or download of such software.

Purchase of Software

The purchase of all software must adhere to this policy.

All purchased software must be purchased by IT Specialist in coordination with Finance Department.

All purchased software must be purchased from reputable software or software license sellers.

All purchases of software must be supported by warranty or support and be compatible with the institution’s server and/or hardware system.

Any changes from the above requirements must be authorised by IT Head Department.

All purchases for software must be in line with the purchasing policy in the Financial policies and procedures manual.

Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from IT

Prosedur

Permintaan Perangkat Lunak

Semua perangkat lunak, termasuk perangkat lunak non-komersial seperti perangkat lunak open source dan freeware disesuaikan berdasarkan kebutuhan. Untuk semua perangkat lunak yang diinstal pada sistem server harus disetujui oleh Spesialis TI sebelum menggunakan atau mengunduh perangkat lunak tersebut.

Pembelian Perangkat Lunak

Pembelian semua perangkat lunak harus mematuhi kebijakan ini.

Semua perangkat lunak yang dibeli harus dibeli oleh Spesialis TI berkoordinasi dengan Departemen Keuangan.

Semua perangkat lunak yang dibeli harus dibeli dari penjual perangkat lunak atau lisensi perangkat lunak yang memiliki reputasi baik.

Semua pembelian perangkat lunak harus didukung oleh garansi atau dukungan dan kompatibel dengan server institusi dan / atau sistem perangkat keras.

Setiap perubahan dari persyaratan di atas harus disahkan oleh Kepala Departemen TI.

Semua pembelian untuk perangkat lunak harus sejalan dengan kebijakan pembelian dalam manual kebijakan dan prosedur Keuangan.

Penerimaan perangkat lunak sumber terbuka atau freeware

Perangkat lunak open source atau freeware dapat diperoleh tanpa pembayaran dan biasanya diunduh langsung dari internet.

Specialist must be obtained only for server systems and must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the institution's hardware and software systems.

Any changes from the above requirements must be authorised by IT Head Department.

Policy for Use of Software

Policy Number: RPC-A003
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the institution to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

Software Licensing

All software copyrights and terms of all software licenses will be forwarded by all employees of the institution.

Where licensing states limited usage (i.e. number of computer or users etc.), then it is the responsibility of IT Specialist to ensure these terms are followed.

Dalam hal diperlukan perangkat lunak sumber terbuka atau freeware, persetujuan dari IT

Spesialis harus diperoleh hanya untuk sistem server dan harus diperoleh sebelum pengunduhan atau penggunaan perangkat lunak tersebut.

Semua open source atau freeware harus kompatibel dengan sistem perangkat keras dan perangkat lunak institusi.

Setiap perubahan dari persyaratan di atas harus disahkan oleh Kepala Departemen TI.

Kebijakan Penggunaan Perangkat Lunak

Nomor kebijakan: RPC-A003
Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk penggunaan perangkat lunak untuk semua karyawan di dalam institusi untuk memastikan bahwa semua penggunaan perangkat lunak sesuai. Di bawah kebijakan ini, penggunaan semua perangkat lunak open source dan freeware akan dilakukan berdasarkan prosedur yang sama yang diuraikan untuk perangkat lunak komersial.

Prosedur

Lisensi Perangkat Lunak

Semua hak cipta dan ketentuan perangkat lunak dari semua lisensi perangkat lunak akan diteruskan oleh semua karyawan lembaga.

IT Specialist is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and license agreements are adhered to.

Software Installation

All software must be appropriately registered with the supplier where this is requirement.

Ritase is to be the registered owner of all software.

Only software obtained in accordance with the getting software policy is to be installed on the institution's computer or server systems.

All software installations is to be carried out by IT Specialist.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the getting software policy is to be used within the institution.

Prior to the use of any software, the employee must receive instructions of any licensing agreements relating to the software, including any restrictions on use of the software.

All employee related must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be responsibility of IT Department.

Jika lisensi menyatakan penggunaan terbatas (mis. Jumlah komputer atau pengguna, dll.), Maka merupakan tanggung jawab Spesialis TI untuk memastikan ketentuan ini dipatuhi.

Spesialis IT bertanggung jawab untuk menyelesaikan audit perangkat lunak semua perangkat keras dua kali setahun untuk memastikan bahwa hak cipta perangkat lunak dan perjanjian lisensi dipatuhi.

Instalasi Perangkat Lunak

Semua perangkat lunak harus terdaftar secara tepat dengan pemasok di mana ini merupakan persyaratan.

Ritase harus menjadi pemilik terdaftar semua perangkat lunak.

Hanya perangkat lunak yang diperoleh sesuai dengan kebijakan perangkat lunak yang akan diinstal pada komputer atau sistem server lembaga.

Semua instalasi perangkat lunak harus dilakukan oleh Spesialis TI.

Pembaruan perangkat lunak tidak boleh diinstal pada komputer yang belum memiliki salinan versi asli perangkat lunak yang dimuat di dalamnya.

Penggunaan Perangkat Lunak

Hanya perangkat lunak yang dibeli sesuai dengan kebijakan perangkat lunak yang dapat digunakan untuk didalam institusi.

Sebelum menggunakan perangkat lunak apa pun, karyawan harus menerima instruksi dari perjanjian lisensi apa pun yang terkait dengan perangkat lunak tersebut, termasuk segala pembatasan penggunaan perangkat lunak tersebut.

Employees are prohibited from using software from home and loading onto institution's server system or infrastructure.

Unless express approval from IT Head Department is obtained, software cannot be taken home or loaded on employee's computer.

Unauthorised software is prohibited from being used in the institution. This includes the use of software owned by an employee and used within the institution.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to employee Head for further consultation or reprimand action. The illegal duplication of software or other copyrighted works is not condoned within this institution and IT Head Department is authorised to undertake disciplinary action where such event occurs.

Breach of Policy

Where there is a breach of this policy by an employee, that employee will be referred to employee Head for further consultation or reprimand action.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify IT Head Department immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to employee Head for further consultation or reprimand action.

Semua karyawan yang terkait harus menerima pelatihan untuk semua perangkat lunak baru. Ini termasuk karyawan baru yang akan dilatih untuk menggunakan perangkat lunak yang ada dengan tepat. Ini akan menjadi tanggung jawab Departemen TI.

Karyawan dilarang menggunakan perangkat lunak dari rumah dan memuat ke sistem server atau infrastruktur lembaga.

Kecuali diperoleh persetujuan tegas dari Kepala Departemen TI, perangkat lunak tidak dapat dibawa pulang atau dimuat di komputer karyawan.

Perangkat lunak yang tidak sah dilarang digunakan di institusi. Hal ini termasuk penggunaan perangkat lunak yang dimiliki oleh karyawan dan digunakan di dalam institusi.

Duplikasi, memperoleh atau menggunakan salinan perangkat lunak yang tidak sah dilarang. Setiap karyawan yang membuat, memperoleh, atau menggunakan salinan perangkat lunak yang tidak sah akan dirujuk ke Kepala Karyawan untuk konsultasi lebih lanjut atau tindakan teguran. Duplikasi ilegal perangkat lunak atau karya berhak cipta lainnya tidak dibenarkan dalam lembaga ini dan Kepala Departemen TI berwenang untuk melakukan tindakan disipliner di mana peristiwa tersebut terjadi.

Pelanggaran Kebijakan

Jika ada pelanggaran kebijakan oleh karyawan, karyawan tersebut akan dirujuk ke Kepala karyawan untuk konsultasi lebih lanjut atau tindakan teguran.

Jika seorang karyawan mengetahui adanya pelanggaran penggunaan perangkat lunak sesuai dengan kebijakan ini, mereka berkewajiban untuk segera memberi tahu Kepala Departemen TI.

Bring Your Own Device Policy

Policy Number: RPC-A004
Policy Date: 15 January 2018

At Ritase we acknowledge the importance of mobile technologies in improving institution communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to Ritase's network and equipment. We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smartphones, tablets and other devices for institution purposes. All staff who use or access Ritase's technology equipment and/or services are bound by the conditions of this policy.

Procedures

Current mobile devices approved for institution use

The following personally owned mobile devices are approved to be used for institution purposes.

- Any notebooks that can open internal Ritase's software and services that used or owned by Ritase.
- Any mobile devices that can open internal Ritase's software and services that used or owned by Ritase.

Dalam hal pelanggaran tidak dilaporkan dan ditetapkan bahwa seorang karyawan gagal melaporkan pelanggaran tersebut, maka karyawan tersebut akan dirujuk ke Kepala karyawan untuk konsultasi lebih lanjut atau tindakan teguran.

Kebijakan Membawa Perangkat Sendiri

Nomor kebijakan: RPC-A004
Tanggal disahkan: 15 Januari 2018

Di Ritase kami mengakui pentingnya teknologi seluler dalam meningkatkan komunikasi dan produktivitas lembaga. Selain meningkatnya penggunaan perangkat seluler, anggota staf telah meminta opsi untuk menghubungkan perangkat seluler mereka sendiri ke jaringan dan peralatan Ritase. Kami mendorong Anda untuk membaca dokumen ini secara penuh dan untuk bertindak berdasarkan rekomendasi. Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk penggunaan notebook, smartphone, tablet, dan perangkat lain yang dimiliki secara pribadi untuk keperluan institusi. Semua staf yang menggunakan atau mengakses peralatan teknologi dan / atau layanan Ritase terikat oleh ketentuan kebijakan ini.

Prosedur

Perangkat seluler saat ini disetujui untuk digunakan di institusi

Perangkat seluler milik pribadi berikut ini disetujui untuk digunakan untuk tujuan institusi.

For all software owned by Ritase and accessed by notebooks or mobile devices must be accessed with employee user account along with its authorisation.

Registration of system user account for institution use

Employees when using personal devices and access software owned by Ritase will register system user account relevant with job title or department.

IT Department will record the user account and all application access used.

Term of mobile devices for institution use

Each employee who utilise personal mobile devices agrees:

- Not to download or transfer institution or personal sensitive information to the device. Sensitive information includes institution intellectual property, employee details, institution statistics and data.
- Not to use the registered mobile devices as the sole repository for Ritase's information. All institution information stored on mobile devices should be backed up.
- To make every reasonable effort to ensure that Ritase's information is not compromised through the use of mobile equipment in a public space. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected.
- To maintain the device with mobile devices such as current operating software and software security.

- Setiap buku catatan yang dapat membuka perangkat lunak dan layanan Ritase internal yang digunakan atau dimiliki oleh Ritase.
- Perangkat seluler apa pun yang dapat membuka perangkat lunak dan layanan Ritase internal yang digunakan atau dimiliki oleh Ritase.

Untuk semua perangkat lunak yang dimiliki oleh Ritase dan diakses oleh notebook atau perangkat seluler harus diakses dengan akun pengguna karyawan bersama dengan otorisasi.

Pendaftaran Akun Pengguna Sistem untuk Penggunaan Institusi

Karyawan ketika menggunakan perangkat pribadi dan mengakses perangkat lunak yang dimiliki oleh Ritase akan mendaftarkan akun pengguna sistem yang relevan dengan jabatan atau departemen pekerjaan.

Departemen TI akan mencatat akun pengguna dan semua akses aplikasi yang digunakan.

Jangka waktu perangkat seluler untuk penggunaan institusi

Setiap karyawan yang menggunakan perangkat seluler pribadi setuju:

- Tidak mengunduh atau mentransfer informasi sensitif pribadi atau perusahaan ke perangkat. Informasi sensitif termasuk properti intelektual institusi, detail karyawan, statistik dan data institusi.
- Tidak menggunakan perangkat seluler terdaftar sebagai satu-satunya tempat penyimpanan untuk informasi Ritase. Semua informasi institusi yang disimpan di perangkat seluler harus didukung.

- To abide by Ritase's internet policy for appropriate use and access of internet sites.
- To notify Ritase immediately in the event of loss or theft of the registered device.

All employees who have a registered personal mobile devices for institution use acknowledge that the institution:

- Owns all intellectual property created on the device related to institution works.
- Can access all data held only for institution intellectual property.
- Will regularly backup data held on device.
- Will delete all data held on the device in the event of loss or theft of the device.
- Has first right to buy the device where the employee wants to sell the device.
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from backup data.
- Has the right to deregister the device for institution use at any time.

Keeping mobile devices secure.

The following must be observed when handling mobile computing devices (such as notebooks
and mobile phones):

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a

- Melakukan segala upaya yang wajar untuk memastikan bahwa informasi Ritase tidak dikompromikan melalui penggunaan peralatan seluler di ruang publik. Layar yang menampilkan informasi sensitif atau kritis tidak boleh dilihat oleh orang yang tidak berwenang dan semua perangkat yang terdaftar harus dilindungi kata sandi.
- Untuk memelihara perangkat dengan perangkat seluler seperti perangkat lunak operasi saat ini dan keamanan perangkat lunak.
- Untuk mematuhi kebijakan internet Ritase untuk penggunaan yang tepat dan akses situs internet.
- Untuk segera memberi tahu Ritase jika terjadi kehilangan atau pencurian perangkat yang terdaftar.

Semua karyawan yang memiliki perangkat seluler pribadi terdaftar untuk penggunaan di institusi mengakui bahwa institusi:

- Memiliki semua kekayaan intelektual yang dibuat pada perangkat yang terkait dengan pekerjaan institusi.
- Dapat mengakses semua data yang dimiliki hanya untuk kekayaan intelektual institusi.
- Akan secara teratur mencadangkan data yang disimpan pada perangkat.
- Akan menghapus semua data yang disimpan pada perangkat jika terjadi kehilangan atau pencurian perangkat.
- Memiliki hak pertama untuk membeli perangkat tempat karyawan ingin menjual perangkat tersebut.
- Akan menghapus semua data yang tersimpan di perangkat setelah pemutusan hubungan kerja karyawan. Karyawan yang diberhentikan dapat meminta data pribadi untuk dipulihkan dari data cadangan.
- Memiliki hak untuk membatalkan pendaftaran perangkat untuk digunakan di institusi kapan saja.

seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Breach of this policy

Any breach of this policy will be referred to employee Head who will review the breach and determine adequate consequences.

Information Technology Security Policy

Policy Number: RPC-A005
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the institution to ensure integrity, confidentiality and availability of data and assets.

Procedures

Physical or System Infrastructure Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access.

It will be the responsibility of IT Specialist to ensure that this requirement is followed at all times. Any employee becoming aware of a

Menjaga Keamanan Perangkat Seluler

Hal-hal berikut harus diperhatikan ketika menangani perangkat komputasi seluler (seperti notebook dan ponsel):

- Perangkat komputer seluler tidak boleh dibiarkan tanpa pengawasan di tempat umum, atau di rumah yang tidak terkunci, atau di kendaraan bermotor, meskipun terkunci. Sedapat mungkin mereka harus disimpan pada orang tersebut atau dikunci dengan aman
- Perangkat penguncian kabel juga harus dipertimbangkan untuk digunakan dengan komputer laptop di tempat umum, mis. dalam seminar atau konferensi, bahkan ketika laptop dihadiri
- Perangkat seluler harus dibawa sebagai tas jinjing saat bepergian dengan pesawat terbang.

Pelanggaran terhadap Kebijakan

pelanggaran kebijakan ini akan dirujuk ke Kepala karyawan yang akan meninjau pelanggaran tersebut dan menentukan konsekuensi yang memadai.

Kebijakan Keamanan Teknologi Informasi

Nomor kebijakan: RPC-A005
Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk perlindungan dan penggunaan aset dan sumber daya teknologi informasi di dalam institusi untuk memastikan integritas, kerahasiaan, dan ketersediaan data dan aset.

breach to this security requirement is obliged to notify IT Head Department immediately.

All security and safety of all portable technology such as notebooks or mobile devices will be the responsibility of the employee who has been issued with the devices. Each employee
is required to use password and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, IT Head Department will assess the security measures undertaken to determine if the employee will be required to reimburse the institution for the loss or damage.

All mobile devices when kept at the office desk is to be secured by password.

Information Security

All sensitive, valuable, or critical institution data or provide a checklist of all data is to be backed-up.

It is the responsibility of IT Department to ensure that data backups are conducted regularly and the backed up data is kept in the cloud.

All technology that has internet access must have anti-virus software installed. It is the
responsibility of employee to install all anti-virus software and ensure that this software remains up to date on all technology used by the institution.

All information used within the institution is to adhere to the privacy laws and the institution's confidentiality requirements. Any employee breaching this will be reported to employee Head.

Prosedur

Keamanan Infrastruktur fisik atau sistem

Untuk semua server, kerangka utama dan aset jaringan lainnya, area tersebut harus diamankan dengan ventilasi yang memadai dan akses yang sesuai.

Hal ini akan menjadi tanggung jawab Spesialis TI untuk memastikan bahwa persyaratan ini dipatuhi setiap saat. Setiap karyawan yang menyadari adanya pelanggaran terhadap persyaratan keamanan ini wajib segera memberi tahu Kepala Departemen TI.

Semua keamanan dan keselamatan semua teknologi portabel seperti notebook atau perangkat seluler akan menjadi tanggung jawab karyawan yang telah dikeluarkan bersama perangkat tersebut. Setiap karyawan diperlukan untuk menggunakan kata sandi dan untuk memastikan aset disimpan dengan aman setiap saat untuk melindungi keamanan aset yang diberikan kepada mereka.

Jika terjadi kehilangan atau kerusakan, Kepala Departemen TI akan menilai langkah-langkah keamanan dilakukan untuk menentukan apakah karyawan akan diminta untuk mengembalikan lembaga atas kehilangan atau kerusakan.

Semua perangkat seluler saat disimpan di meja kantor harus diamankan dengan kata sandi.

Informasi Keamanan

Semua data institusi yang sensitif, berharga, atau kritis atau memberikan daftar periksa semua data harus dicadangkan.

Technology Access

Every employee will be issued with a unique identification code to access the institution technology and will be required to set a password for access.

Each password is to be a number of alpha and numeric and is not to be shared with any employee within the institution.

IT Specialist is responsible for the issuing of the identification code and initial password for all employees.

Adalah tanggung jawab Departemen TI untuk memastikan bahwa pencadangan data dilakukan secara teratur dan data yang dicadangkan disimpan di cloud.

Semua teknologi yang memiliki akses internet harus sudah menginstal perangkat lunak anti-virus. Ini adalah

tanggung jawab karyawan untuk menginstal semua perangkat lunak anti-virus dan memastikan bahwa perangkat lunak ini tetap terkini pada semua teknologi yang digunakan oleh institusi.

Semua informasi yang digunakan dalam institusi adalah untuk mematuhi undang-undang privasi dan institusi

persyaratan kerahasiaan. Setiap karyawan yang melanggar hal ini akan dilaporkan kepada Kepala karyawan.

Akses Teknologi

Setiap karyawan akan diberikan kode identifikasi unik untuk mengakses institusi teknologi dan akan diminta untuk mengatur kata sandi untuk akses.

Setiap kata sandi harus berupa angka alfa dan angka dan tidak boleh dibagikan dengan karyawan mana pun di dalam lembaga.

Spesialis TI bertanggung jawab atas penerbitan kode identifikasi dan kata sandi awal untuk semua karyawan.

The following table provides the authorisation of access:

Enrollment	Type	Person authorised for access
GSuite for Business	Email platform	IT Head Department
Godaddy	Domain	IT Head Department
Amazon Web Services	Infrastructure	IT Head Department or IT Specialist
Gitlab	Code repository	IT Head Department or IT Specialist
Slack	Communication	All employees
stichdata.com	ETL	IT Specialist and Data Team
JIRA + Confluence	Project Management	IT Department
DocuSign	Legal	IT Specialist and Legal
Midtrans	Payment Gateway	IT Specialist and Finance
Disbursement	Midtrans Iris (sandbox)	IT Specialist and Finance
Zeplin	Design prototyping	IT Department
Continuous Integration	Jenkins	IT Department
Docusign	signing documents	IT Specialist and Legal
elasticemail.com	Email marketing & campaign	IT Department and Marketing
Zendesk	support & knowledge based	IT Department and Control Tower
Invision	Sketch UI/UX	IT Department
NeverBounce	Email verification	IT Department
Youtube	video	IT Department and Marketing
Ekrut	recruitment	IT Department and Human Resources
airtable	spreadsheet API-able	IT Department
Balsamiq	Prototyping	IT Department
Indoreg	domain	IT Head Department
Facebook	Social media	IT Department and Marketing
Instagram	Social media	IT Department and Marketing
Youtube	Social media	IT Department and Marketing
Xero	Finance & Invoice Management	IT Department and Finance

Employees are only authorised to use institution computers for personal use without any breach of other policies.

For internet and social media usage, refer to the Human Resources Manual.

It is the responsibility of IT Head Department to keep all procedures for this policy up to date.

Information Technology Administration Policy

Policy Number: RPC-A006
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the institution.

Procedures

All software installed and the license information must be registered on the specific documents. It is the responsibility of IT Head Department to ensure that this registrations is maintained. The register must record the following information:

- What software is installed on every machine
- What license agreements are in place for each software package
- Renewal dates if applicable

IT Specialist is responsible for the maintenance and management of all service agreements for the institution technology. Any

Karyawan hanya diberi wewenang untuk menggunakan komputer institusi untuk penggunaan pribadi tanpa melanggar kebijakan lainnya.

Untuk penggunaan internet dan media sosial, lihat Manual Sumber Daya Manusia.

Kepala Departemen TI bertanggung jawab untuk memperbarui semua prosedur kebijakan ini.

Kebijakan Administrasi Teknologi Informasi

Nomor kebijakan: RPC-A006
Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk administrasi aset dan sumber daya teknologi informasi di dalam institusi.

Prosedur

Semua perangkat lunak yang diinstal dan informasi lisensi harus didaftarkan pada dokumen spesifik. Kepala Departemen TI bertanggung jawab untuk memastikan pendaftaran ini tetap terjaga. Register harus mencatat informasi berikut:

- Perangkat lunak apa yang diinstal pada setiap mesin
- Apa perjanjian lisensi yang berlaku untuk setiap paket perangkat lunak
- Tanggal pembaruan jika berlaku

Spesialis TI bertanggung jawab atas pemeliharaan dan pengelolaan semua perjanjian layanan untuk teknologi institusi. Setiap persyaratan layanan harus terlebih dahulu disetujui oleh Kepala Departemen TI.

service requirements must first be approved by IT Head Department.

IT Specialist is responsible for maintaining adequate technology spare parts and system infrastructure.

A technology audit is to be conducted regularly by IT Specialist to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to IT Head Department.

Website Policy

Policy Number: RPC-A007
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the institution website.

Procedures

Website Register

The website register must record the following details:

- List of domain names registered to the institution
- Date of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

Spesialis TI bertanggung jawab untuk memelihara suku cadang teknologi yang memadai dan infrastruktur sistem.

Audit teknologi akan dilakukan secara berkala oleh Spesialis TI untuk memastikan bahwa semua kebijakan teknologi informasi dipatuhi.

Segala persyaratan administrasi teknologi yang tidak ditentukan harus diarahkan ke Kepala Departemen TI.

Kebijakan Situs Web

Nomor Kebijakan: RPC-A007
Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk pemeliharaan semua masalah teknologi terkait yang terkait dengan situs web institusi.

Prosedur

Pendaftaran Situs Web

pendaftaran situs web harus mencatat rincian berikut:

- Daftar nama domain yang terdaftar di institusi
- Tanggal pembaruan untuk nama domain
- Daftar penyedia layanan hosting
- Tanggal kedaluwarsa hosting

Menjaga agar daftar selalu diperbarui akan menjadi tanggung jawab Spesialis TI.

Spesialis IT akan bertanggung jawab atas setiap pembaruan barang yang terdaftar dalam register.

The keeping the register up to date will be the responsibility of IT Specialist.

IT Specialist will be responsible for any renewal of items listed in the register.

Website Content

All content of the institution website is to be accurate, appropriate and current. This will be the responsibility of IT Department.

All content on the website must follow institution content plan.

The content of the website is to be reviewed regularly.

The following persons are authorised to make changes to the institution website.

- IT Specialist
- Marketing
- Legal
- Human Resources

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the institution.

All data collected from the website is to adhere to the Privacy Art.

Electronic Transactions Policy

Policy Number: RPC-A008
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Konten Situs Web

Semua konten situs web institusi harus akurat, tepat, dan terkini. Ini akan menjadi tanggung jawab Departemen TI.

Semua konten di situs web harus mengikuti rencana konten institusi.

Konten situs web akan ditinjau secara berkala.

Orang-orang berikut berwenang untuk membuat perubahan pada situs web institusi.

- Spesialis IT
- Pemasaran
- Legal
- Sumber Daya Manusia

Pedoman branding dasar harus diikuti di situs web untuk memastikan citra yang konsisten dan kohesif bagi institusi.

Semua data yang dikumpulkan dari situs web adalah untuk mematuhi Seni Privasi.

Kebijakan Transaksi Elektronik

Nomor Kebijakan: RPC-A008
Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk semua transaksi elektronik yang dilakukan atas nama institusi.

Tujuan kebijakan ini adalah untuk memastikan transfer dan penerimaan dana elektronik dimulai, dilaksanakan, dan disetujui secara aman.

Purpose of the Policy

This policy provides guidelines for the all electronic transactions undertaken on behalf of the institution.

The objective of this policy is to ensure of electronics funds transfers and receipts are started, carried out, and approved in a secure manner.

Procedures

Electronic Funds Transfer (EFT)

It is the policy of Ritase that all payments and receipts should be made by EFT where appropriate.

All EFT payments and receipts must adhere to all finance policies in the Financial Policies and Procedures Manual.

All EFT arrangements, including receipts and payments must be submitted to Finance Department.

EFT payments must have the appropriate authorisation for payment in line with the financial transactions policy in the Financial Policies and Procedures Manual.

EFT payments must be appropriately recorded in line with the financial policy in the Financial Policies and Procedures Manual.

EFT payment sonce authorised, will be entered into internal finance payment system by Finance Department.

EFT payments can only be released for payment once pending payments have been authorised by Finance Department.

Prosedur

Transfer Dana Elektronik (TDE)

Merupakan kebijakan Ritase bahwa semua pembayaran dan penerimaan harus dilakukan dengan TDE jika perlu.

Semua pembayaran dan penerimaan TDE harus mematuhi semua kebijakan keuangan dalam Manual Kebijakan dan Prosedur Keuangan.

Semua pengaturan TDE, termasuk tanda terima dan pembayaran harus diserahkan ke Departemen Keuangan.

Pembayaran TDE harus memiliki otorisasi yang sesuai untuk pembayaran sejalan dengan kebijakan transaksi keuangan dalam Manual Kebijakan dan Prosedur Keuangan.

Pembayaran TDE harus dicatat secara tepat sesuai dengan kebijakan keuangan dalam Manual Kebijakan dan Prosedur Keuangan.

Pembayaran TDE resmi, akan dimasukkan ke dalam sistem pembayaran keuangan internal oleh Departemen Keuangan.

Pembayaran TDE hanya dapat dirilis untuk pembayaran setelah pembayaran yang tertunda telah disahkan oleh Departemen Keuangan.

Untuk kontrol yang baik atas pembayaran TDE, pastikan bahwa orang yang mengotorisasi pembayaran dan melakukan pembayaran bukan orang yang sama.

Semua tanda terima TDE harus direkonsiliasi ke catatan pelanggan seminggu sekali.

For good control over EFT payments, ensure that the persons authorising the payments and
making the payment are not the same person.

All EFT receipts must be reconciled to customer records once a week.

Where EFT receipt cannot be allocated to customer account, it is responsibility of Finance Department to investigate. In the event that the customer account cannot be identified
within one month the receipted funds must be returned to source. Finance Department must authorise this transaction.

It is the responsibility of Finance Department to annually review EFT authorisations for
initial entry, alterations, or deletion of EFT records, including supplier payment records and
customer receipt records.

Electronic Purchases

All electronic purchases by any authorised employee must adhere to the purchasing policy in the Financial Policies and Procedures Manual.

Where an electronic purchase is being considered, the person authorising this transaction must ensure that the internet sales site is secure and safe and be able to demonstrate that this has been reviewed.

All electronic purchases must be undertaken using institution credit cards only and therefore
adhere to the institution credit card policy in the Financial

Jika tanda terima TDE tidak dapat dialokasikan ke akun pelanggan, Departemen Keuangan bertanggung jawab untuk menyelidikinya. Dalam hal akun pelanggan tidak dapat diidentifikasi dalam satu bulan dana yang diterima harus dikembalikan ke sumber. Departemen Keuangan harus mengesahkan transaksi ini.

Departemen Keuangan bertanggung jawab untuk meninjau otorisasi TDE setiap tahun entri awal, perubahan, atau penghapusan catatan EFT, termasuk catatan pembayaran pemasok dan catatan penerimaan pelanggan.

Pembelian Elektronik

Semua pembelian elektronik oleh karyawan yang berwenang harus mematuhi kebijakan pembelian dalam Manual Kebijakan dan Prosedur Keuangan.

Di mana pembelian elektronik sedang dipertimbangkan, orang yang mengesahkan transaksi ini harus memastikan bahwa situs penjualan internet aman dan aman dan dapat menunjukkan bahwa ini telah ditinjau.

Semua pembelian elektronik harus dilakukan hanya dengan menggunakan kartu kredit institusi dan karenanya mematuhi kebijakan kartu kredit institusi dalam Keuangan

Kebijakan Perjanjian Layanan TI

Nomor Kebijakan: RPC-A009
Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

IT Service Agreements Policy

Policy Number: RPC-A009
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the institution.

Procedures

The following IT service agreements can be entered into on behalf of the institution:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of institution software
- Provision of mobile phones and relevant plans
- Website design, maintenance etc.

All IT service agreements must be reviewed by Legal Department before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by institution.

All IT service agreements, obligations and renewals must be recorded at specific documents.

Where an IT service agreement renewal is required, in the event that the agreement is

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk semua perjanjian layanan TI yang dibuat atas nama institusi.

Prosedur

Perjanjian layanan TI berikut ini dapat dibuat atas nama institusi:

- Penyediaan layanan TI umum
- Penyediaan perangkat keras dan lunak jaringan
- Perbaikan dan perawatan peralatan TI
- Penyediaan perangkat lunak institusi
- Penyediaan ponsel dan rencana yang relevan
- Desain situs web, pemeliharaan, dll.

Semua perjanjian layanan TI harus ditinjau oleh Departemen Hukum sebelum perjanjian tersebut dibuat. Setelah perjanjian ditinjau dan rekomendasi untuk eksekusi diterima, maka perjanjian harus disetujui oleh institusi.

Semua perjanjian, kewajiban, dan pembaruan layanan TI harus dicatat pada dokumen tertentu.

Di mana pembaruan perjanjian layanan TI diperlukan, dalam hal perjanjian itu secara substansial tidak berubah dari perjanjian sebelumnya, maka pembaruan perjanjian ini bisa disahkan oleh Kepala Departemen TI.

Di mana pembaruan perjanjian layanan TI diperlukan, dalam hal perjanjian itu memiliki secara substansial berubah dari perjanjian sebelumnya, Departemen Hukum sebelum perpanjangan dibuat. Setelah perjanjian ditinjau dan rekomendasi untuk eksekusi diterima, maka perjanjian harus disetujui oleh institusi.

substantially unchanged from the previous agreement, then this agreement renewal can be
authorised by IT Head Department.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, Legal Department before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by institution.

In the event that there is a dispute to the provision of IT services covered by an IT service
agreement, it must be referred to IT Head Department who will be responsible for the settlement of such dispute.

Emergency Management of Information Technology

Policy Number: RPC-A010
Policy Date: 15 January 2018

This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the institution.

Dalam hal terjadi perselisihan dengan penyediaan layanan TI yang dicakup oleh layanan Perjanjian TY, harus dirujuk ke IT Head Department yang akan bertanggung jawab untuk penyelesaian perselisihan tersebut.

Manajemen Darurat Teknologi Informasi

Nomor Kebijakan: RPC-A010
Tanggal disahkan: 15 Januari 2018

Kebijakan ini harus dibaca dan dilakukan oleh semua staf.

Tujuan Kebijakan

Kebijakan ini memberikan pedoman untuk manajemen darurat semua teknologi informasi di dalam institusi.

Prosedur

Kegagalan Perangkat Keras TI

Jika ada kegagalan pada salah satu perangkat keras institusi, ini harus segera dirujuk ke Departemen TI.

Adalah tanggung jawab Departemen TI untuk menangani masalah ini jika terjadi kegagalan perangkat keras TI.

Adalah tanggung jawab Departemen TI untuk melakukan tes pada prosedur darurat yang direncanakan sebulan sekali untuk memastikan bahwa semua prosedur darurat yang direncanakan sesuai dan meminimalkan gangguan pada operasi institusi.

Virus atau Pelanggaran Keamanan Lainnya

Procedures

IT Hardware Failure

Where there is failure of any of the institution's hardware, this must be referred to IT Department immediately.

It is the responsibility of IT Department to handle this issue in the event of IT hardware failure.

It is the responsibility of IT Department to undertake tests on planned emergency procedures once a month to ensure that all planned emergency procedures are appropriate and minimise disruption to institution operations.

Virus or other security breach

In the event that the institution's information technology is compromised by software virus or
other relevant possible security breaches such breaches are to be reported to IT Specialist immediately.

IT Specialist is responsible for ensuring that any security breach is dealt with
within hours to minimise disruption to institution operations.

Website Disruption

In the event that institution website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- IT Specialist must be notified immediately
- IT Specialist take DRP and BCP action

Dalam hal teknologi informasi institusi dikompromikan oleh virus perangkat lunak atau pelanggaran keamanan lain yang relevan yang mungkin terjadi, pelanggaran tersebut harus segera dilaporkan kepada Spesialis TI.

Spesialis TI bertanggung jawab untuk memastikan bahwa setiap pelanggaran keamanan ditangani dalam beberapa jam untuk meminimalkan gangguan pada operasi institusi.

Gangguan Situs Web

Jika situs web institusi terganggu, tindakan berikut harus segera dilakukan:

- Host situs web akan diberitahukan
- Spesialis IT harus segera diberitahukan
- Spesialis TI mengambil tindakan DRP dan BCP