OfficialUMT

BEKERJA DARI RUMAH (BDR)

GARIS PANDUAN

KAEDAH PELAKSANAAN BEKERJA DARI RUMAH (BDR) UNIVERSITI MALAYSIA TERENGGANU

KUATKUASA 1 JANUARI 2025

Kelulusan Mesyuarat JKSM Kali Ke-32 Bil. 3 Tahun 2024

KANDUNGAN

GARIS PANDUAN PELAKSANAAN

BEKERJA DARI RUMAH (BDR)

BAHAGIAN A

PELAKSANAAN

Objektif

1. Garis Panduan ini bertujuan untuk menjelaskan tatacara pelaksanaan Bekerja Dari Rumah (BDR) di UMT.

Prinsip Pelaksanaan BDR

2. Pegawai Universiti hanya boleh BDR apabila :
   (a) mendapat arahan daripada Kerajaan atau Ketua Setiausaha Negara atau Ketua Pengarah Perkhidmatan Awam (tempoh tertakluk kepada arahan yang dikeluarkan); atau
   (b) mendapat arahan atau kebenaran daripada Pendaftar.

Tujuan BDR

3. Arahan BDR boleh dipertimbangkan bagi tujuan seperti berikut :

Kategori	Kenyataan/Situasi
Kesihatan	a. Pegawai mengalami masalah kesihatan untuk bergerak dari rumah ke tempat kerja (kampus induk/kampus cawangan). Pengesahan masalah kesihatan hendaklah disahkan oleh pegawai perubatan Kerajaan/Pusat Kesihatan Pelajar (PKU), UMT. b. Sekiranya pegawai hendak menjaga ahli keluarga yang sakit (meliputi keluarga pegawai sendiri (isteri/suami dan anak-anak), ibu bapa, adik-beradik, ibu bapa mertua, nenek dan datuk pegawai), pegawai hendaklah memohon cuti separuh gaji.

Keselamatan	a. Untuk mengurangi atau mengelakkan kerugian/kerosakan/kemusnahan atas sebab-sebab seperti pencemaran alam sekitar, penularan penyakit berjangkit dan/atau bencana alam yang boleh mengancam keselamatan, ketenteraman awam sama ada di pejabat/premis Universiti atau kawasan tempat kediaman. b. Pegawai tidak dapat menghadirkan diri ke pejabat kerana kawasan kediaman pegawai termasuk dalam kawasan yang dikenakan perintah kawalan pergerakan atau lain-lain tindakan yang menyebabkan terhalang pergerakan pegawai; c. Pejabat pegawai Universiti diwartakan oleh Kerajaan sebagai Pusat Kuarantin atau lain-lain kegunaan bagi menangani isu-isu tertentu.
Bangunan pejabat/dalaman pejabat	a. Pejabat pegawai Universiti perlu dikosongkan kerana, antara lain, mengalami serangan kulat/serangga atau kerosakan struktur bangunan/premis/pejabat. b. Kerja-kerja penyelenggaraan/pengubahsuaian bangunan/pejabat yang menganggu kerja-kerja hakiki pegawai ("workstation" / bilik pegawai).
Mewujudkan keseimbangan dan kesejahteraan antara keperluan universiti terhadap kesinambungan tugas demi kepentingan perkhidmatan dan keperluan pegawai menguruskan hal persendirian. Pelaksanaan BDR atas dasar ini boleh dilaksanakan bagi skop tugasan yang munasabah.	a. Antara contoh situasi/keadaan tersebut adalah seperti keperluan untuk menjaga anak-anak yang berusia 12 tahun dan ke bawah akibat penutupan taska/pusat asuhan kanak-kanak/sekolah rendah disebabkan, antara lain, atas arahan Kerajaan. b. Antara contoh skop tugasan yang munasabah pula ialah tugasan yang boleh dilaksanakan secara dalam talian atau memerlukan pemantauan yang minimum atau tugasan yang tidak melibatkan urusan teknikal di lapangan dengan kehadiran secara bersemuka. c. Perkhidmatan-perkhidmatan kritikal yang ditentukan oleh Universiti juga tidak dibenarkan BDR atau dilaksanakan secara bergilir jika ada keperluan.
Mengelakkan berlaku kemudaratan, kesukaran atau keadaan serba salah sama ada terhadap pegawai Universiti atau mana-mana pegawai-pegawai lain di pejabat sekiranya pegawai Universiti berkenaan hadir di pejabat	Antara contoh situasi/keadaan tersebut adalah seperti kehadiran pegawai di pejabat boleh menyebabkan wujudnya percanggahan kepentingan peribadi (*conflict of interest*) yang memungkinkan, antara lain, kebocoran maklumat atau membawa penglibatan pengaruh luar.

Kaedah Pelaksanaan

4. Kaedah pelaksanaan BDR adalah seperti berikut :-

   4.1. Kerajaan atau Pendaftar boleh mempertimbangkan sama ada semua, sebahagian atau mana-mana pegawai Universiti untuk BDR;

   4.2. Arahan daripada Kerajaan boleh dibuat dengan menggunakan apa-apa saluran komunikasi rasmi Kerajaan atau suatu pemakluman oleh Jabatan Perkhidmatan Awam;

   4.3. Ketua Pusat Tanggungjawab boleh mempertimbangkan arahan BDR kepada pegawai Universiti menggunakan borang Arahan Bekerja Dari Rumah seperti di **Lampiran A** tertakluk kepada kelulusan Pendaftar; dan

   4.4. Ketua Pusat Tanggungjawab hendaklah memastikan semua arahan Kerajaan dan Universiti yang dikeluarkan dipatuhi pelaksanaannya di peringkat Pusat Tanggungjawab masing-masing.

5. Sekiranya tiada arahan rasmi yang lain, Ketua Pusat Tanggungjawab boleh melaksanakan ketetapan kuota kehadiran di pejabat dalam menghadapi situasi-situasi yang membenarkan pegawai Universiti BDR.

Kriteria Pegawai

6. Kriteria pegawai Universiti yang layak dipertimbangkan BDR adalah seperti berikut :-

   6.1. Arahan Kerajaan atau Ketua Setiausaha Negara atau Ketua Pengarah Perkhidmatan Awam

      6.1.1. Semua, sebahagian atau mana-mana pegawai Universiti kecuali mana-mana perkhidmatan, kumpulan atau kategori yang ditetapkan Kerajaan sebaliknya.

      6.1.2. Tertakluk kepada arahan Kerajaan atau Ketua Setiausaha Negara atau Ketua Pengarah Perkhidmatan Awam, Pendaftar hendaklah

menentukan perkhidmatan penting (*essential services*) bagi memastikan kesinambungan perkhidmatan Universiti. Sebagai contoh, perkhidmatan yang boleh diberikan pengecualian BDR ialah kepada pegawai Universiti yang;

(i) bekerja di lapangan sepanjang tempoh waktu bekerjanya; atau

(ii) berurusan secara terus dengan orang ramai atau kumpulan sasar sama ada di kaunter perkhidmatan, atau lain-lain yang seumpama dengannya.

6.2. Arahan Pendaftar

6.2.1. BDR layak dipertimbangkan kepada mana-mana pegawai Universiti.

6.3 Arahan Ketua Pusat Tanggungjawab

6.3.1 BDR layak dipertimbangkan kepada mana-mana pegawai Universiti tertakluk kepada kelulusan Pendaftar.

6.3.2 Tempoh BDR yang boleh diluluskan tertakluk kepada kepentingan perkhidmatan.

BAHAGIAN B

WAKTU BEKERJA, HARI, TEMPOH DAN TEMPAT SEMASA BDR

Waktu Bekerja

1. Waktu bekerja pegawai Universiti yang melaksanakan BDR adalah mengikut waktu bekerjanya sama ada waktu bekerja pejabat, waktu bekerja bukan pejabat atau waktu-waktu bekerja yang lain mengikut sesuatu perkhidmatan.

2. Pegawai Universiti hendaklah mematuhi waktu bekerjanya sama ada waktu bekerja pejabat, waktu bekerja bukan pejabat atau waktu bekerja yang lain mengikut sesuatu perkhidmatan.

3. BDR boleh dilaksanakan dengan dua (2) kaedah seperti yang berikut :

   (a) "BDR Sepenuh Hari" bermaksud pegawai Universiti melaksanakan tugas hakiki atau tugas-tugas rasmi lain di Rumah mengikut waktu kerjanya yang telah ditetapkan kepada pegawai Universiti.

   (b) "BDR Separuh Hari" bermaksud pegawai Universiti melaksanakan tugas hakiki atau tugas-tugas rasmi lain di Rumah mengikut waktu kerjanya yang telah ditetapkan kepada pegawai Universiti dengan *cut off* waktu rehat dengan baki tempoh separuhnya, pegawai Universiti dikehendaki bertugas di pejabat atau lain-lain lokasi yang diarahkan oleh Ketua Pusat Tanggungjawab. Jumlah waktu bekerja di pejabat dan di rumah hendaklah mengikut ketetapan Universiti (tidak termasuk waktu rehat).

Hari BDR

4. BDR boleh dilaksanakan untuk sesuatu tempoh tertentu dan boleh dibuat secara giliran atau bukan giliran mengikut hari atau mingguan.

5. Peraturan semasa mengenai Hari Rehat Mingguan, Hari Kelepasan Mingguan dan Hari Kelepasan Am adalah terpakai dalam penggunaan BDR ini.

Tempoh BDR

6. Tempoh BDR adalah tertakluk kepada arahan yang dikeluarkan oleh Kerajaan, atau Ketua Setiausaha Negara atau Ketua Pengarah Perkhidmatan Awam atau Pendaftar atau Ketua Pusat Tanggungjawab.

Tempat Bekerja

7. Tempat bekerja pegawai Universiti semasa BDR ialah Rumah.

8. Rumah adalah kediaman pegawai Universiti seperti alamat tempat tinggal yang didaftarkan dengan Pejabat Pendaftar.

9. Pegawai hendaklah sentiasa mengemaskini alamat rumah kediaman bagi tujuan BDR.

10. Ketua Pusat Tanggungjawab boleh mengarahkan pegawai Universiti untuk menghadiri mesyuarat rasmi di pejabat atau di suatu lokasi lain semasa BDR.

11. Sekiranya pegawai hendak meninggalkan pejabatnya (Rumah) di dalam waktu bekerja, kebenaran Pegawai Penyelia hendaklah diperolehi terlebih dahulu sebelum berbuat demikian.

BAHAGIAN C

GAJI, ELAUN, KEMUDAHAN DAN SKIM PERLINDUNGAN

Gaji, Elaun dan Kemudahan

1. Kelayakan gaji pegawai Universiti Universiti yang BDR tidak terjejas dan masih tertakluk kepada peraturan semasa yang berkuat kuasa.

2. Pegawai Universiti yang BDR layak menikmati semua jenis elaun dan kemudahan yang diperuntukkan mengikut syarat dan peraturan semasa yang berkuat kuasa kecuali yang dinyatakan sebaliknya.

3. Elaun Lebih Masa (ELM) adalah tidak layak dibayar kepada pegawai Universiti yang BDR. Sekiranya, pegawai Universiti BDR diarahkan bekerja di lokasi lain selain Rumah di luar waktu bekerjanya, ELM boleh dipertimbangkan tertakluk kepada peraturan yang berkuat kuasa.

4. Kerajaan dan Universiti tidak akan menanggung apa-apa kos utiliti seperti bil telefon, bil elektrik, sewaan jalur lebar, pembaikan kerosakan peralatan dan sebagainya sepanjang tempoh pegawai Universiti BDR.

5. Bagi tujuan tuntutan elaun, kemudahan dan bayaran kerana menjalankan tugas rasmi semasa BDR hendaklah mematuhi semua Pekeliling Perbendaharaan dan peraturan kewangan yang ditetapkan oleh Universiti.

Skim Perlindungan Untuk Pegawai Yang BDR

6. Pegawai Universiti yang diarahkan BDR adalah layak dipertimbangkan bayaran faedah Skim *Ex-Gratia* Bencana Kerja sekiranya mengalami bencana sehingga menyebabkan hilang upaya kekal atau kematian semasa menjalankan tugas di Rumah dalam tempoh waktu bekerja yang ditetapkan.

7. Syarat dan peraturan pemberian pampasan Skim Ex-Gratia Bencana Kerja adalah

tertakluk kepada pekeliling, surat pekeliling, surat edaran dan arahan oleh Kementerian Kewangan yang berkuat kuasa dari semasa ke semasa.

BAHAGIAN D

KEMUDAHAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (TMK)

Kemudahan Infrastruktur dan Digital Peralatan Atau Peranti TMK

1. Peralatan dan peranti TMK merupakan keperluan asas untuk menjalankan tugasan di Rumah. Sehubungan itu, beberapa tindakan boleh diambil seperti berikut :-

    1.1. pegawai Universiti hendaklah mempunyai peranti mudah alih seperti telefon pintar dan kemudahan capaian internet yang sewajarnya;

    1.2. Pusat Ekosistem Digital (PED) boleh berdasarkan keperluan, membekalkan peralatan dan peranti TMK yang bersesuaian kepada pegawai Universiti. Antara peralatan dan peranti tersebut adalah komputer riba, peranti mudah alih (contoh: *tablet*) atau lain-lain perkakasan yang berkaitan. Peralatan atau peranti TMK yang berkaitan perlu dilengkapi dengan perisian yang sesuai untuk melancarkan pelaksanaan tugasan harian. Walau bagaimanapun, penggunaan peralatan atau perkakasan persendirian boleh dibenarkan dengan syarat mematuhi kriteria keselamatan dan disahkan oleh Pengarah Pusat Ekosistem Digital (PED).

    1.3. Peralatan yang berkaitan dengan sewaan masih lagi tertakluk kepada perjanjian sewaan sedia ada sehingga dimaklumkan sebaliknya.

    1.4. Pusat Ekosistem Digital (PED) hendaklah memastikan peralatan atau peranti TMK yang berkaitan dilindungi dari kod hasad dengan memasang perisian *Endpoint Detection And Response* (EDR), atau sekurang-kurangnya perisian antivirus yang dapat mengesan kod hasad dan *ransomware* secara *real-time.*

    1.5. Pusat Ekosistem Digital (PED) hendaklah mengeluarkan arahan pentadbiran yang membenarkan pegawai membawa pulang peralatan atau peranti TMK yang diperlukan sekiranya pegawai menggunakan peralatan atau peranti milik

Universiti;

1.6. Pusat Ekosistem Digital (PED) tidak akan membekalkan perkakasan-perkakasan lain seperti mesin pencetak, mesin fotostat, mesin pengimbas dan mesin perincih. Sekiranya pegawai Universiti perlu menggunakan perkakasan-perkakasan ini, pegawai Universiti perlu hadir ke pejabat;

1.7. Pusat Ekosistem Digital (PED) perlu menyediakan Prosedur Operasi Standard (SOP) bagi menjaga keselamatan peralatan atau peranti TMK dengan merujuk kepada Dasar dan Peraturan ICT dan Polisi Keselamatan Siber (PKS) UMT.

1.8. Setiap pegawai Universiti hendaklah mengambil langkah-langkah yang bersesuaian bagi memastikan keselamatan peralatan atau peranti TMK yang dibekalkan oleh Universiti berdasarkan SOP yang ditetapkan.

Sistem Pengurusan Kehadiran Pegawai

2. Sistem kehadiran bekerja universiti (*MyTime*) pegawai Universiti bertujuan untuk merekod kehadiran (waktu masuk dan waktu pulang) dan tempoh masa bekerja menggunakan *MyTime* tanpa mengambil kira kehadiran pegawai Universiti ke stesen kerja fizikal. Universiti boleh menggunakan *MyTime* yang merekod kehadiran bertugas, merekod lokasi pegawai, memuat naik data kehadiran, menguruskan kehadiran pegawai, merekod catatan tugas pegawai, memantau tugasan pegawai di bawah seliaan, memuat turun kehadiran, menjana laporan dan statistik kehadiran.

Pengesahan Identiti Pegawai

3. Semua sistem aplikasi dan kawalan capaian sumber TMK Universiti yang berkaitan hendaklah mengambil kira keperluan pengesahan identiti pegawai Universiti dan diubahsuai mengikut tahap keselamatan perlindungan yang sewajarnya.

4. Pengesahan identiti pegawai Universiti bertujuan untuk menentukan kesahihan identiti pegawai Universiti bagi mengelakkan penipuan identiti dan penyalahgunaan

sumber Kerajaan dan Universiti. Antara kaedah pengesahan identiti pegawai yang boleh dipertimbang untuk diguna pakai adalah menggunakan kemudahan *single sign-on*.

Capaian Atau Akses Kepada Sumber

5. Semasa BDR, terdapat keperluan untuk pegawai Universiti mengakses sumber TMK universiti bagi melaksanakan tugasan rasmi. Universiti hendaklah mengambil langkah-langkah yang perlu bagi memastikan kebenaran capaian tidak mengkompromi aspek keselamatan sumber TMK tersebut.

6. Capaian hanya dibenarkan dalam persekitaran komunikasi selamat dan mendapat kelulusan Pengarah Pusat Ekosistem Digital (PED). *Access Control List* (ACL) kepada sumber TMK bagi capaian jarak jauh perlu diperketat dan dipantau penggunaannya. Penggunaan kaedah capaian menggunakan *tunnelling* berasaskan *Secure Sockets Layer Virtual Private Network* (SSLVPN) hendaklah dilaksanakan bagi capaian langsung yang membenarkan pengemaskinian.

Pemantauan Secara Maya Bagi Sasaran Kerja dan Output

7. Bagi tujuan pemantauan secara maya yang lebih berkesan, Universiti boleh membangun dan menggunakan Sistem Aplikasi Diari BDR, seumpama Diari Rasmi bagi membolehkan pegawai merekodkan aktiviti kerja yang dilaksanakan semasa BDR atau lain-lain aplikasi yang seumpamanya. Ketua Pusat Tanggungjawab atau penyelia boleh menyemak dan mengesahkan diari ini secara berkala serta boleh menjadi input kepada semakan semula sasaran kerja dan output.

Penyeliaan Tugasan Pegawai Secara Digital

8. Ketua Pusat Tanggungjawab atau penyelia hendaklah sentiasa menyelia tugasan pegawai Universiti BDR bertujuan untuk memantau status dan perkembangan tugasan pegawai yang telah ditetapkan.

9. Universiti boleh mengguna apa-apa saluran komunikasi yang bersesuaian dan selamat seperti telesidang, *instant messaging*, perkongsian dokumen, pengurusan mesyuarat secara maya serta perkongsian *desktop,* bagi memastikan tugasan pegawai Universiti menepati kehendak atau sasaran yang ditetapkan.

Pengurusan Dokumen Universiti

10. Dokumen dan data Universiti perlu diurus dengan lebih sistematik bagi melindungi maklumat Universiti. Sehubungan itu, Universiti boleh mengguna pakai kemudahan aplikasi dan perkhidmatan yang telah disediakan oleh Universiti mengikut tatacara yang berkuat kuasa dari semasa ke semasa.

11. Selain daripada itu, pegawai Universiti perlu memastikan maklumat terperingkat diproses pada peralatan atau peranti TMK yang dibekalkan atau dibenarkan oleh Universiti sahaja. Pegawai Universiti tidak dibenarkan berkongsi dokumen terperingkat Kerajaan dan Universiti di platform media sosial seperti *Whatsapp, Facebook* dan sebagainya. Hanya maklumat umum seperti sebaran maklumat, infografik dan perbincangan umum dibenarkan untuk dikongsi di platform media sosial. Selain daripada itu, pegawai Universiti juga tidak dibenarkan berkongsi dokumen terperingkat Kerajaan dan Universiti pada rangkaian yang tidak dipercayai. (contoh: *public wi-fi*).

Pengendalian, Pengurusan dan Pemantauan Mesyuarat Secara Digital

12. Sepanjang tempoh BDR, mesyuarat boleh dijalankan secara maya dengan mengambil kira perkara-perkara berikut :-

    12.1. Universiti boleh mengguna pakai perkhidmatan telesidang untuk mengadakan mesyuarat secara maya. Bagi keselamatan data, kawalan keselamatan diperketatkan di mana data *in transit* dikawal dengan kaedah penyulitan data dan saluran komunikasi dilindungi dengan ciri-ciri keselamatan yang dipertingkatkan;

12.2. sebarang bentuk mesyuarat Universiti boleh mengguna pakai Sistem Mesyuarat Universiti (e-Meeting) untuk mengurus dan memantau mesyuarat secara digital. Sistem Mesyuarat Universiti (e-Meeting) mematuhi prosedur kitaran pengurusan mesyuarat iaitu persediaan sebelum mesyuarat, penyediaan minit dan maklum balas serta pemantauan keputusan mesyuarat. Sistem ini turut dilengkapi dengan ciri-ciri keselamatan (kawalan capaian dan penyulitan data) bagi memastikan maklumat Universiti adalah terjamin;

12.3. telesidang hendaklah mengadaptasi teknik yang selamat seperti penggunaan kata laluan sebelum dibenarkan terlibat di dalam telesidang berkenaan; dan

12.4. merekodkan telesidang tersebut (jika perlu) dan rekod hendaklah disimpan di dalam storan komputer pengguna.

Pengurusan Perkhidmatan dan Pelaksanaan Urusan Kerja Yang Berkesan

13. Pengurusan perkhidmatan dan pelaksanaan urusan kerja yang berkesan adalah bagi memastikan urusan perkhidmatan disediakan secara menyeluruh dan memudah cara setiap tugasan dalam aliran kerja aplikasi spesifik yang ditetapkan. Sehubungan itu, beberapa tindakan yang boleh diambil adalah:

13.1. Pusat Tanggungjawab hendaklah menyediakan aliran kerja digital yang menyeluruh bagi memudahkan urusan kerja pegawai Universiti;

13.2. Pejabat Pendaftar hendaklah memperkasakan penggunaan aplikasi dalam talian bagi semua urusan perkhidmatan Universiti;

13.3. Pusat Tanggungjawab hendaklah memastikan tugasan pegawai Universiti dalam aliran kerja aplikasi spesifik dilaksanakan pada persekitaran digital yang kondusif dan menyeluruh; dan

13.4. Pusat Ekosistem Digital (PED) hendaklah memastikan pembangunan sistem

adalah secara pendekatan *thin-client* atau *web-based* di mana semua sumber ditempatkan di persekitaran *server* dan tidak di *local hard disk* pegawai. Ini dapat meningkatkan prestasi pembangunan sistem tanpa bergantung kepada spesifikasi peralatan TMK yang dibekalkan kepada pegawai.

Ekosistem Digital Yang Selamat

1. Ekosistem digital yang selamat perlu mengambil kira semua elemen keselamatan melibatkan sumber manusia, proses dan teknologi. Langkah-langkah yang perlu diambil tindakan untuk memastikan ekosistem digital yang selamat bagi menyokong BDR adalah seperti di **Lampiran B.**

2. Universiti juga perlu mematuhi semua akta, dasar dan garis panduan yang berkuat kuasa untuk menjamin keselamatan ekosistem digital. Sehubungan itu, sebarang insiden keselamatan TMK hendaklah dilaporkan kepada Agensi Keselamatan Siber Negara (NACSA) melalui Ketua Pegawai Maklumat Universiti.

Pertanyaan

3. Sebarang pertanyaan berkaitan Kemudahan Teknologi Maklumat dan Komunikasi (TMK), bolehlah dirujuk kepada Ketua Pegawai Maklumat Universiti/Pengarah Pusat Ekosistem Digital (PED).

BAHAGIAN E

PEMATUHAN PERATURAN

Peraturan Pegawai Universiti

1. Pegawai Universiti yang diarahkan BDR adalah tertakluk kepada semua peraturan yang berkuat kuasa, termasuklah apa-apa pekeliling perkhidmatan, surat pekeliling perkhidmatan, surat edaran atau apa-apa arahan lain yang dikeluarkan oleh Kerajaan dan Universiti dari semasa ke semasa.

2. Pegawai Universiti boleh dikenakan tindakan tatatertib sekiranya tidak mematuhi syarat dan peraturan yang telah ditetapkan. Pendaftar, tertakluk kepada persetujuan Ketua Pusat Tanggungjawab, boleh menamatkan arahan atau kebenaran BDR yang diberikan kepada pegawai Universiti dengan serta-merta sekiranya pegawai Universiti didapati melanggar syarat dan peraturan yang telah ditetapkan.

3. Pegawai Universiti diambil kira sebagai hadir bekerja apabila hadir pada hari, tempat dan tempoh di mana pegawai Universiti diarahkan BDR untuk melaksanakan tugasan yang ditetapkan.

4. Ketidakhadiran bertugas tanpa cuti atau tanpa terlebih dahulu mendapat kebenaran atau tanpa sebab yang munasabah boleh menyebabkan pegawai dikenakan tindakan tatatertib mengikut Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000 *[Akta 605.*

5. Ketua Pusat Tanggungjawab bertanggungjawab menjalankan kawalan, pemantauan dan pengawasan tatatertib ke atas pegawai Universiti yang BDR. Kegagalan Ketua Pusat Tanggungjawab berbuat demikian dianggap sebagai cuai dalam melaksanakan tugasnya dan boleh dikenakan tindakan tatatertib berdasarkan kepada Peraturan 21, Bahagian I, Peraturan-peraturan Tatatertib Badan-badan Berkanun, Jadual Kedua, Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000 *[Akta 605].*

Keselamatan Peralatan Hak Milik Universiti

6. Pegawai Universiti bertanggungjawab untuk menjaga keselamatan peralatan yang disediakan selaras dengan garis panduan yang ditetapkan oleh Universiti. Sekiranya pegawai Universiti gagal menjaga aset Kerajaan dan Universiti sehingga mengakibatkan kehilangan atau kerosakan aset tersebut, pegawai boleh dikenakan tindakan surcaj seperti yang diperuntukkan di bawah Akta Tatacara Kewangan 1957 [*Akta 61*] atau apa-apa tindakan lain mengikut peraturan yang berkuat kuasa.

7. Kerajaan tidak akan bertanggungjawab ke atas sebarang kerosakan dan kemusnahan ruang atau peralatan persendirian yang digunakan oleh pegawai Universiti yang disebabkan oleh kecuaian pegawai Universiti ketika menjalankan tugas rasmi di Rumah.

8. Sebarang kehilangan atau kerosakan yang berlaku terhadap harta Kerajaan hendaklah dilaporkan dengan segera kepada Ketua Pusat Tanggungjawab atau pihak-pihak yang berkenaan mengikut peraturan-peraturan yang berkuat kuasa.

Kerahsiaan Dokumen Rasmi

9. Sekiranya kerja-kerja pegawai Universiti melibatkan dokumen terperingkat, langkah-langkah pengurusan dan perlindungan hendaklah diambil sebagaimana ditetapkan oleh Universiti.

10. Pegawai Universiti bertanggungjawab untuk menjaga kerahsiaan dokumen Kerajaan dan Universiti dan hendaklah memastikan semua dokumen Kerajaan dan Universiti sama ada dalam bentuk salinan cetak dan salinan elektronik disimpan dengan sempurna dan diletakkan di tempat yang selamat serta mematuhi kehendak Akta Rahsia Rasmi 1972 [*Akta 88*], Arahan Keselamatan dan apa-apa peraturan, pekeliling, garis panduan atau arahan yang dikeluarkan oleh Kerajaan dan Universiti dari semasa ke semasa.

11. Dokumen terperingkat tidak dibenarkan dibuka di tempat-tempat awam kecuali dengan kebenaran oleh Universiti.

12. Pegawai Universiti dipertanggungjawabkan sepenuhnya untuk menjaga kerahsiaan kata laluan dan memastikan semua peralatan TMK dimatikan (*log off*) apabila tidak digunakan.

Lampiran A

UMT/PEND/BDR (2024)

UNIVERSITI MALAYSIA TERENGGANU
PEJABAT PENDAFTAR
Aras 2, Bangunan Canselori dan Pentadbiran
21030 Kuala Nerus, Terengganu Darul Iman
Tel. : 09-668 4342/4824/4906 Faks : 09-669 6441

ARAHAN BEKERJA DARI RUMAH (BDR)

BAHAGIAN I : BUTIRAN DIRI PEGAWAI

1. Nama Penuh : _____
2. No. Staf UMT : _____
3. Jawatan & Gred : _____
4. PTJ : _____
5. No. Telefon : _____

Tarikh : _____

_____
(Tandatangan dan Cap Jabatan)

BAHAGIAN II : ARAHAN DARIPADA KETUA PUSAT TANGGUNG JAWAB

Tuan/Puan diarahkan untuk Bekerja Dari Rumah dan hendaklah melaksanakan tugas-tugas berikut:

1. _____
2. _____
3. _____

Tarikh / Tempoh	:		Hingga :		Jumlah hari bekerja	
Alamat Semasa BDR	:					
Peminjaman Peralatan PTJ (Jika ada)	:					

Tarikh : _____

_____
(Tandatangan dan Cap Jabatan)

BAHAGIAN III : KELULUSAN PENDAFTAR

Arahan BDR ini **DILULUSKAN/TIDAK DILULUSKAN**
Ulasan (Jika ada):

_____

_____

Tarikh : _____

_____
(Tandatangan dan Cap Jabatan)

LAMPIRAN B

LANGKAH KAWALAN KESELAMATAN EKOSISTEM DIGITAL BAGI MENYOKONG PELAKSANAAN BEKERJA DARI RUMAH

Bil.	Perkara	Keterangan
1.	Membudayakan amalan baik kawalan keselamatan dalam Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)	Panduan asas kepada Jabatan dalam merancang perlindungan keselamatan maklumat yang diperlukan bagi ruang siber Jabatan masing-masing. Antara kawalan keselamatan Bekerja Dari Rumah yang perlu diberi perhatian adalah seperti berikut :-
	(a) Keselamatan peranti pemprosesan maklumat	i. Memastikan sistem pengoperasian dan semua aplikasi yang digunakan adalah sah dan dilengkapi dengan *security patches* yang terkini; ii. Memastikan peranti dilindungi dari kod hasad dengan memasang perisian *Endpoint Detection And Response* (EDR), atau sekurang-kurangnya perisian antivirus yang dapat mengesan kod hasad dan *ransomware* secara *real-time*; iii. Melaksanakan penyulitan kepada media storan bagi mengurangkan risiko capaian tidak sah ke atas maklumat jika berlaku kecurian; iv. Melaksanakan imbasan kod hasad pada media storan mudah alih sebelum sebarang aktiviti dilaksanakan berkaitan media storan berkenaan; v. Melaksanakan sandaran (*backup*) bagi data dan maklumat Kerajaan untuk mengurangkan risiko data tidak dapat di akses jika berlaku kerosakan peranti; vi. Melaksanakan keselamatan fizikal bagi mengurangkan risiko kecurian dan kerosakan peranti; vii. Melaksanakan *screen lock* jika tidak berada di hadapan komputer/peranti; viii. Mengasingkan komputer yang digunakan untuk maklumat rasmi dan urusan peribadi; dan ix. Menggunakan *secure delete* jika perlu memadamkan fail.
	(b) Mengendalikan maklumat terperingkat	i. Memastikan maklumat terperingkat diproses pada perkakasan atau peranti TMK yang dibekalkan oleh Kerajaan sahaja; ii. Menggunakan teknologi penyulitan jika ingin memindahkan maklumat menggunakan e-mel, media storan mudah alih atau lain-lain medium yang sesuai; dan iii. Peranti yang digunakan untuk memproses maklumat terperingkat tidak boleh disambungkan ke rangkaian

Bil.	Perkara	Keterangan
		yang tidak dipercayai (contoh: *public wi-fi*).
	(c) Capaian ke atas sistem aplikasi dalaman Jabatan	Menggunakan VPN yang disediakan oleh Jabatan masing-masing bagi capaian ke atas sistem aplikasi dalaman Jabatan.
	(d) Capaian ke atas *server* Jabatan bagi pentadbir sistem	Menggunakan perisian *Priviledge Access Management* (PAM) atau yang setara bagi capaian ke atas *server* dan peralatan rangkaian Jabatan untuk tujuan penyelenggaraan dan lain-lain tugas yang berkaitan.
	(e) Sambungan ke atas rangkaian komputer di rumah	i. Menggunakan medium yang selamat (contoh: kabel UTP) bagi sambungan ke atas rangkaian komputer dan internet; ii. Sekiranya menggunakan wi-fi, konfigurasi *Wireless Access Point* (WAP) hendaklah menggunakan teknologi penyulitan yang terkini (contoh: WPA2 atau yang terkini); dan *iii.* Menggunakan router yang bebas dari sebarang *security vulnerabilities.*
	(f) Pengesahan identiti pengguna	i. Menggunakan kata laluan yang selamat/kukuh dan perlu ditukar secara berkala; dan ii. Menggunakan *Multi Factor Authentication* (MFA) - jika disediakan.
	(g) Komunikasi telesidang	i. Menggunakan telesidang, perkhidmatan di bawah MyGovUC2.0; ii. Mengadaptasi teknik yang selamat, seperti penggunaan kata laluan sebelum dibenarkan terlibat di dalam telesidang berkenaan; dan iii. Menyimpan rekod di dalam storan komputer pengguna (dan bukannya di *public cloud*), sekiranya komunikasi persidangan perlu direkod.
	(h) Program kesedaran pengguna berkenaan ancaman keselamatan maklumat	Mendedahkan pengguna dengan risiko ancaman keselamatan maklumat seperti *social engineering* dan sebagainya terutamanya yang melibatkan isu semasa.
	(i) Pelaporan insiden keselamatan TMK	Sebarang insiden keselamatan TMK hendaklah dilaporkan kepada Agensi KeseSlamatan Siber Negara (NACSA) melalui Ketua Pegawai Maklumat Universiti.