

## BAB V

### KESIMPULAN DAN SARAN

#### 5.1. Kesimpulan

Berdasarkan hasil dari penelitian yang dilakukan untuk mengukur kesadaran keamanan informasi yang dimiliki oleh karyawan Bank BTN Kantor Cabang Solo didapatkan kesimpulan bahwa responden atau karyawan Bank BTN Kantor Cabang Solo sudah memahami dan sadar bagaimana cara untuk menjaga keamanan informasi. Tingkat *Information Security Awareness* (ISA) yang dimiliki oleh subjek penelitian sudah cukup baik hal ini dapat dilihat dari hasil kuesioner, hasil perhitungan kesadaran keamanan informasi dan hasil wawancara. Dari fokus area yang diukur lebih dari 50% karyawan memiliki respon yang baik dimana mereka memiliki pengetahuan yang baik, sikap yang baik dan perilaku yang baik. Hanya saja masih memiliki beberapa aspek yang perlu ditingkatkan baik dari segi kebijakan keamanan informasi perusahaan maupun tingkat pemahaman dan pengetahuan individu yang dimiliki oleh karyawan Bank BTN Kantor Cabang Solo.

Fokus area yang perlu ditingkatkan dilihat dari fokus area yang bernilai rendah. Beberapa nilai fokus area yang bernilai rendah terdapat pada fokus area “Pelaporan Insiden” dengan sub-area “Mengabaikan tindakan mencurigakan dari rekan kerja” ( $M=5,38$ ), pada fokus area “Penggunaan Perangkat *Mobile*” dengan sub area “Perlindungan fisik” ( $M=6,76$ ), dan yang terakhir pada fokus area “Manajemen *Password*” dengan sub area “Membagikan *Password*” ( $M=6,86$ ). Solusi yang dapat digunakan untuk meningkatkan *Information Security Awareness* (ISA) pada subjek penelitian yaitu melakukan perbaikan kebijakan dan prosedur terkait dengan fokus area yang bernilai rendah. Selain itu melakukan pelatihan keamanan informasi dapat meningkatkan pemahaman dan pengetahuan individu terkait dengan keamanan informasi.

#### 5.2. Saran

Hasil penelitian ini diharapkan dapat berguna untuk acuan studi dan penelitian serupa dengan fokus yang berbeda dikemudian hari. Masih terdapat beberapa batasan atau kekurangan yang ada pada penelitian ini, seperti isi dari pada kuesioner yang mungkin kedepannya dapat ditingkatkan dan dikembangkan agar mendapatkan hasil penelitian yang memuaskan. Pendekatan kepada responden juga diperlukan agar hasil dari pada data yang didapat lebih akurat, kurangnya penulis dalam melakukan wawancara terhadap responden mungkin mempengaruhi hasil dari penelitian.

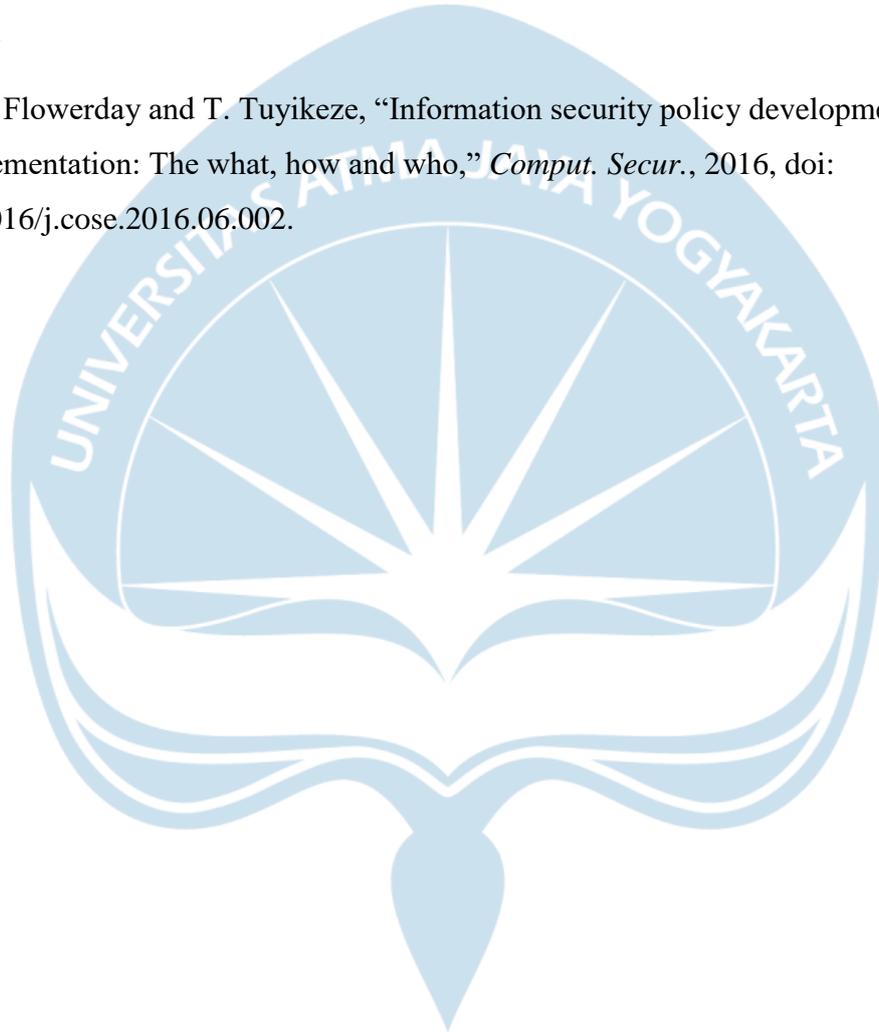
## Daftar Pustaka

- [1] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.
- [2] L. Jaeger, "Information Security Awareness: Literature Review and Integrative Framework," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018, doi: 10.24251/hicss.2018.593.
- [3] L. Cronk, "Culture's influence on behavior: Steps toward a theory," *Evol. Behav. Sci.*, 2017, doi: 10.1037/ebs0000069.
- [4] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput. Secur.*, 2020, doi: 10.1016/j.cose.2019.101640.
- [5] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, 2014, doi: 10.1016/j.cose.2013.12.003.
- [6] A. Zulfia, R. Adawiyah, A. N. Hidayanto, and N. Fitriah Ayuning Budi, "Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS," *5th Int. Conf. Comput. Eng. Des. ICCED 2019*, 2019, doi: 10.1109/ICCED46541.2019.9161120.
- [7] I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," *J. Comput. Inf. Syst.*, vol. 0, no. 00, pp. 1–12, 2019, doi: 10.1080/08874417.2019.1650676.
- [8] M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, and C. Jerram, "Examining attitudes toward information security behaviour using mixed methods," in *Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015*, 2015.
- [9] A. Cindana and Y. Ruldeviyani, "Measuring information security awareness on

- employee using HAIS-Q: Case study at XYZ firm,” *2018 Int. Conf. Adv. Comput. Sci. Inf. Syst. ICACSYS 2018*, pp. 289–294, 2019, doi: 10.1109/ICACSYS.2018.8618219.
- [10] N. S. Safa and R. Von Solms, “An information security knowledge sharing model in organizations,” *Comput. Human Behav.*, vol. 57, pp. 442–451, 2016, doi: 10.1016/j.chb.2015.12.037.
- [11] A. McCormac, D. Calic, K. Parsons, T. Zwaans, M. Butavicius, and M. Pattinson, “Test-retest reliability and internal consistency of the human aspects of information security questionnaire (HAIS-Q),” *Proc. 27th Australas. Conf. Inf. Syst. ACIS 2016*, 2016.
- [12] M. Amin, “Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (McdA),” *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, pp. 15–24, 2014.
- [13] T. Galba, K. Solic, and I. Lukic, “An information security and privacy self-assessment (ISPSA) tool for internet users,” *Acta Polytech. Hungarica*, 2015, doi: 10.12700/aph.12.7.2015.7.9.
- [14] S. Egelman, M. Harbach, and E. Peer, “Behavior ever follows intention?: A validation of the Security Behavior Intentions Scale (SeBIS),” in *Conference on Human Factors in Computing Systems - Proceedings*, 2016, doi: 10.1145/2858036.2858265.
- [15] G. Öütücü, Ö. M. Testik, and O. Chouseinoglou, “Analysis of personal information security behavior and awareness,” *Comput. Secur.*, 2016, doi: 10.1016/j.cose.2015.10.002.
- [16] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “The development of the human aspects of information security questionnaire (HAIS-Q),” *Proc. 24th Australas. Conf. Inf. Syst.*, 2013.
- [17] M. Syahril Iskandar, “Metode Deskriptif,” *Metod. Deskriptif*, 2020.
- [18] S. Suliyanto, “Metode Penelitian Kuantitatif,” *Penelit. Kuantitatif*, 2017.
- [19] S. Campbell *et al.*, “Purposive sampling: complex or simple? Research case examples,” *J. Res. Nurs.*, 2020, doi: 10.1177/1744987120927206.
- [20] R. F. DeVellis, “Scale Development Theory and Applications (Fourth Edition),” *SAGE*

*Publ.*, 2016.

- [21] R. Akramana, Candiwanb, and Yudi Priyadic, “Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia,” *J. Sist. Inf. Bisnis 02*, 2018.
- [22] C. C. Dian Chisva Islami, Khodijah Bunga I.H, “KESADARAN KEAMANAN INFORMASI PADA PEGAWAI BANK X DI BANDUNG INDONESIA,” *INKOM*, 2016.
- [23] S. V. Flowerday and T. Tuyikeze, “Information security policy development and implementation: The what, how and who,” *Comput. Secur.*, 2016, doi: 10.1016/j.cose.2016.06.002.



## Lampiran Kuesioner

### Human Aspects of Information Security Questionnaire

Berikan tanda centang ( V ) pada kolom nilai (1-5) yang mewakili jawaban anda yang sebenarnya berdasarkan pertanyaan berikut :

1 = Sangat tidak setuju, 5= Sangat setuju

HAIS-Q Item		1	2	3	4	5
Fokus Area: <i>Password</i> Manajemen						
1.	Saya menggunakan <i>password</i> yang sama dengan media sosial untuk akun yang digunakan dalam bekerja					
2.	Saya merasa aman jika menggunakan <i>password</i> yang sama untuk media sosial dan akun yang digunakan dalam bekerja					
3.	Saya menggunakan <i>password</i> yang berbeda untuk media sosial dan akun yang digunakan untuk bekerja					
4.	Saya bersedia membagikan <i>password</i> kepada teman kerja					
5.	Saya merasa membagikan <i>password</i> merupakan ide yang kurang bagus, bahkan ketika teman kerja memintanya					
6.	Saya membagikan <i>password</i> yang saya miliki kepada teman kerja					
7.	Saya merasa perlu menggunakan huruf, simbol, dan angka sebagai kombinasi <i>password</i>					
8.	Saya sudah merasa aman hanya menggunakan huruf dalam kombinasi <i>password</i> yang saya miliki					
9.	Saya sudah menggunakan huruf, simbol, dan angka sebagai kombinasi <i>password</i>					

Fokus Area: Penggunaan E-mail						
1.	Saya setuju untuk mengklik link di <i>email</i> yang berasal dari orang yang saya kenal					
2.	Saya merasa aman untuk mengklik link di <i>email</i> yang berasal dari orang yang saya kenal					
3.	Saya tidak selalu mengklik link di <i>email</i> yang bahkan berasal dari orang yang saya kenal					
4.	Saya tidak diizinkan untuk mengklik link di <i>email</i> yang berasal dari orang yang tidak saya kenal					
5.	Saya merasa tidak akan terjadi apa-apa kalau saya mengklik link di <i>email</i> yang berasal dari orang yang tidak saya kenal					
6.	Jika <i>email</i> yang saya dapat dari orang yang tidak dikenal terlihat menarik, saya langsung mengklik link yang diberikan oleh <i>email</i> tersebut					
7.	Saya setuju untuk membuka lampiran yang disematkan pada <i>email</i> dari orang tidak dikenal					
8.	Saya merasa sangat beresiko jika saya membuka lampiran yang disematkan pada <i>email</i> dari orang tidak dikenal					
9.	Saya tidak akan membuka lampiran yang disematkan pada <i>email</i> jika itu berasal dari orang tidak dikenal					
Fokus Area: Penggunaan Internet						
1.	Saya setuju untuk mendownload semua file pada komputer kerja, jika itu dapat membantu pekerjaan saya					
2.	Saya merasa mendownload file dikomputer kerja saya sangat beresiko					
3.	Saya mendownload semua file yang dapat membantu dalam menyelesaikan pekerjaan saya					

4.	Ketika saya sedang bekerja, sebaiknya saya tidak mengakses <i>website</i> yang meragukan					
5.	Saya merasa hanya karna saya boleh mengakses <i>website</i> saat bekerja, tidak berarti hal tersebut aman untuk dilakukan					
6.	Ketika mengakses internet saat bekerja, saya membuka semua <i>website</i> yang ingin saya buka					
7.	Saya setuju untuk menginputkan informasi pada sebuah <i>website</i> jika itu dapat membantu pekerjaan saya					
8.	Saya merasa jika menginputkan informasi dapat membantu pekerjaan saya, tidak masalah data apa saja yang harus diinputkan pada <i>website</i> tersebut					
9.	Saya memastikan keamanan <i>website</i> sebelum menginput informasi apapun					
Fokus Area: Penggunaan Media Sosial						
1.	Saya harus secara rutin mengecek pengaturan privasi pada media sosial yang saya miliki					
2.	Saya merasa mengecek pengaturan privasi pada media sosial yang saya miliki merupakan hal yang baik					
3.	Saya tidak mengecek pengaturan privasi pada media sosial yang saya miliki					
4.	Saya tidak mungkin diberhentikan dari pekerjaan saya karena sesuatu yang saya post pada media sosial					
5.	Saya merasa tidak masalah jika saya memposting sesuatu yang tidak biasa saya katakan pada publik					
6.	Saya tidak memposting apapun disosial media yang saya miliki sebelum mempertimbangan konsekuensi buruk yang akan diterima					

7.	Saya merasa bisa memposting apapun yang saya mau tentang pekerjaan saya ke media sosial yang saya miliki					
8.	Saya merasa sangat beresiko memposting informasi penting tentang pekerjaan saya ke media sosial					
9.	Saya memposting apapun yang saya inginkan tentang pekerjaan saya ke media sosial					
Fokus area: Penggunaan perangkat <i>mobile</i>						
1.	Ketika bekerja di tempat umum, saya akan membawa laptop saya kemanapun saya pergi					
2.	Ketika bekerja disebuah cafe, saya merasa aman ketika meninggalkan laptop tanpa perlindungan keamanan apapun dalam beberapa menit					
3.	Ketika bekerja ditempat umum, saya meninggalkan laptop saya tanpa perlindungan keamanan apapun					
4.	Saya setuju untuk mengirim file pekerjaan yang sensitif menggunakan Wi-Fi umum					
5.	Saya merasa mengirim file pekerjaan yang sensitif menggunakan Wi-Fi umum sangat beresiko					
6.	Saya mengirim file pekerjaan yang sensitif menggunakan Wi-Fi umum					
7.	Ketika sedang mengerjakan dokumen sensitif, saya harus memastikan bahwa orang lain tidak dapat melihat layar komputer/laptop saya					
8.	Saya merasa sangat beresiko jika orang lain dapat melihat layar komputer/laptop ketika saya sedang mengerjakan dokumen sensitif					
9.	Saya mengecek dan memastikan bahwa orang lain tidak dapat melihat layar komputer/laptop					

	saya ketika saya sedang mengerjakan dokumen sensitif					
Fokus Area: Penanganan Informasi						
1.	File sensitif dalam bentuk <i>print-out</i> bisa jadi dapat dibuang dengan cara yang sama dengan file biasa					
2.	Saya merasa membuang file sensitif yang berbentuk <i>print-out</i> kedalam tempat sampah aman					
3.	Ketika file sensitif perlu dibuang, saya rasa file perlu dihancurkan atau dibakar					
4.	Jika saya menemukan flashdisk ditempat umum, saya sebaiknya tidak memasangnya pada komputer/laptop saya					
5.	Jika saya menemukan flashdisk ditempat umum, tidak akan ada yang terjadi jika saya memasangnya pada komputer/laptop saya					
6.	Saya tidak akan memasang flashdisk yang saya temukan ditempat umum pada komputer/laptop saya					
7.	Saya setuju untuk meninggalkan <i>print-out</i> file yang mengandung informasi sensitif di meja kantor					
8.	Saya merasa meninggalkan <i>print-out</i> file yang mengandung informasi sensitif di meja kantor sangat beresiko					
9.	Saya meninggalkan <i>print-out</i> file yang mengandung informasi sensitif di meja kantor ketika saya sedang tidak berada dikantor					
Fokus Area: Pelaporan insiden						
1.	Jika seseorang bersikap dengan mencurigakan ditempat kerja saya, saya harus melaporkannya					

2.	Jika saya mengabaikan seseorang yang bersikap mencurigakan ditempat kerja saya, tidak adahal buruk yang akan terjadi					
3.	Jika saya melihat seseorang yang mencurigakan ditempat kerja saya, saya akan melakukan sesuatu untuk itu					
4.	Saya harus mengabaikan perilaku keamanan buruk yang dimiliki teman kerja saya					
5.	Tidak akan ada hal buruk yang akan terjadi jika saya mengabaikan perilaku keamanan buruk yang dimiliki teman kerja saya					
6.	Jika saya melihat teman kerja saya mengabaikan kebijakan keamanan, saya tidak akan melakukan tindakan apapun					
7.	Melaporkan insiden keamanan merupakan sebuah pilihan					
8.	Mengabaikan insiden kemanan sangat beresiko, walaupun jika saya berpikir hal itu tidak berpengaruh					
9.	Jika saya mengetahui insiden keamanan, saya akan melaporkan hal tersebut					

## Tabel Revisi

	Tugas Revisi	Halaman Revisi
1.	Memperbaiki kata “menejemen” menjadi “manajemen”	Mengubah semua kalimat menejemen yang terdapat pada halaman 4, 10, 13, 14, 32 dan 40.
2.	Memperbaiki masalah penelitian pada bagan keterkaitan	Mengubah isi bagan keterkaitan pada halaman 11.
3.	Memperbaiki latar belakang	Manambahkan metode pengukuran kesadaran keamanan informasi selain HAIS-Q
4.	Penambahan rumus pada pembahasan	Menambahkan rumus <i>mean</i> pada halaman 31
5.	Memperbaiki landasan teori	Menambahkan penjelasan HAIS-Q pada halaman 14 dan 15
6.	Memperbaiki rekomendasi	Menambahkan beberapa penjelasan dan referensi pendukung pada halaman 41
7.	Memperbaiki kesimpulan	Menambahkan beberapa penjas terkait dengan “sudah cukup baik” pada halaman 43